10/765,143

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　１月２１日

出願番号
Application Number: 特願２００４－０１２９０４

[ST. 10/C]: [ＪＰ２００４－０１２９０４]

出願人
Applicant(s): 株式会社リコー

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００４年　２月　６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

【書類名】　特許願
【整理番号】　0400503
【提出日】　平成16年 1月21日
【あて先】　特許庁長官　今井　康夫　殿
【国際特許分類】　G03G 21/00　370
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　毛呂井　昭平
【特許出願人】
　【識別番号】　000006747
　【氏名又は名称】　株式会社リコー
【代理人】
　【識別番号】　100070150
　【弁理士】
　【氏名又は名称】　伊東　忠彦
【先の出願に基づく優先権主張】
　【出願番号】　特願2003- 19721
　【出願日】　平成15年 1月29日
【手数料の表示】
　【予納台帳番号】　002989
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9911477

【書類名】特許請求の範囲
【請求項１】
アプリケーションと、当該アプリケーションにシステム側サービスを提供するシステム側ソフトウェアとを有する画像形成装置であって、
認証用画面を前記画像形成装置のオペレーションパネルに表示させ、前記認証用画面から入力された認証用データが認証条件を満たした場合に、前記画像形成装置の使用をするための画面を前記認証用画面に代えて前記オペレーションパネルに表示させる認証モジュールを有し、
当該認証モジュールは、前記システム側ソフトウェアとは別に備えられていることを特徴とする画像形成装置。
【請求項２】
前記システム側ソフトウェアは認証機能部を含み、
利用者により前記画像形成装置における特定のアプリケーションが選択されたときに、前記画像形成装置は、アプリケーションの種類と、前記認証モジュール又は前記システム側ソフトウェアの認証機能部との対応付けを示す情報を参照することにより、前記特定のアプリケーションに対応する前記認証モジュール又は前記システム側ソフトウェアの認証機能部を用いて認証を行う請求項１に記載の画像形成装置。
【請求項３】
前記認証モジュールを前記画像形成装置に外付けされる記録媒体から実行する手段、又は前記認証モジュールを前記記録媒体から前記画像形成装置にロードして実行する手段を有する請求項１又は２に記載の画像形成装置。
【請求項４】
前記認証モジュールを、前記画像形成装置と通信ネットワークを介して接続されたサーバからダウンロードし、実行する認証モジュール実行手段を有する請求項１又は２に記載の画像形成装置。
【請求項５】
前記認証モジュールは、Ｊａｖａ（登録商標）プログラムであり、前記認証モジュール実行手段は、クラスライブラリと仮想マシンを含む請求項４に記載の画像形成装置。
【請求項６】
前記画像形成装置は、携帯端末と無線データ通信を行うための通信手段を更に有し、
前記認証モジュールは、前記通信手段により前記携帯端末から受信した認証用データを用いて認証を行う請求項１又は２に記載の画像形成装置。
【請求項７】
前記画像形成装置は、前記携帯端末から前記認証用データを入力させるための画面データを生成し、当該画面データを前記携帯端末に送信する手段を有する請求項６に記載の画像形成装置。
【請求項８】
前記認証用データとして、部署名又はアプリケーションの使用目的を利用者に入力させる請求項１ないし７のうちいずれか１項に記載の画像形成装置。
【請求項９】
前記認証モジュールの認証用画面を、前記画像形成装置の立ち上がり時に優先的に前記オペレーションパネルに表示させる手段を有する請求項１又は２に記載の画像形成装置。
【請求項１０】
前記オペレーションパネルに前記認証用画面以外の画面を表示しているときに、前記画像形成装置におけるジョブの終了、又は前記画像形成装置のシステムオートクリア、又は前記認証モジュールを使用するためのキー入力がなされた場合に、前記認証用画面以外の画面に代えて前記認証用画面を表示させる手段を有する請求項１又は２に記載の画像形成装置。
【請求項１１】
前記画像形成装置は、所定のジョブが終了した後、一定時間の経過を検出した場合に前

記システムオートクリアを起動し、前記認証用画面を表示する請求項１０に記載の画像形成装置。

【請求項１２】

前記認証モジュールは、前記画像形成装置の利用に関するログ情報を収集する手段を有する請求項１又は２に記載の画像形成装置。

【請求項１３】

前記認証モジュールは、前記利用に関するログ情報として印刷完了通知を収集し、印刷枚数が予め定めた許容枚数に達したときに前記オペレーションパネルに警告表示をさせる請求項１２に記載の画像形成装置。

【請求項１４】

アプリケーションと、当該アプリケーションにシステム側サービスを提供するシステム側ソフトウェアとを有する画像形成装置における認証方法であって、

前記画像形成装置に前記システム側ソフトウェアとは別に認証モジュールを備え、該認証モジュールが、認証用画面を前記画像形成装置のオペレーションパネルに表示させ、前記認証用画面から入力された認証データが認証条件を満たした場合に、前記画像形成装置の使用をするための画面を前記認証用画面に代えて前記オペレーションパネルに表示させることを特徴とする認証方法。

【請求項１５】

前記システム側ソフトウェアは認証機能部を含み、

利用者により前記画像形成装置における特定のアプリケーションが選択されたときに、前記画像形成装置は、アプリケーションの種類と、前記認証モジュール又は前記システム側ソフトウェアの認証機能部との対応付けを示す情報を参照することにより、前記特定のアプリケーションに対応する前記認証モジュール又は前記システム側ソフトウェアの認証機能部を用いて認証を行う請求項１４に記載の認証方法。

【請求項１６】

前記認証モジュールを前記画像形成装置に外付けされる記録媒体から実行、又は前記認証モジュールを前記記録媒体から前記画像形成装置にロードして実行する請求項１４又は１５に記載の認証方法。

【請求項１７】

前記認証モジュールを、前記画像形成装置と通信ネットワークを介して接続されたサーバからダウンロードし、実行する請求項１４又は１５に記載の認証方法。

【請求項１８】

前記画像形成装置は、携帯端末と無線データ通信を行うための通信手段を更に有し、

前記認証モジュールは、前記通信手段により前記携帯端末から受信した認証用データを用いて認証を行う請求項１４又は１５に記載の認証方法。

【請求項１９】

前記画像形成装置は、前記オペレーションパネルに前記認証用画面以外の画面を表示しているときに、前記画像形成装置におけるジョブの終了、又は前記画像形成装置のシステムオートクリア、又は前記認証モジュールを使用するためのキー入力がなされた場合に、前記認証用画面以外の画面に代えて前記認証用画面を表示させる請求項１４又は１５に記載の認証方法。

【請求項２０】

前記認証モジュールは、前記画像形成装置の利用に関するログ情報を収集する請求項１４又は１５に記載の認証方法。

【請求項２１】

アプリケーションと、当該アプリケーションにシステム側サービスを提供するシステム側ソフトウェアとを有する画像形成装置に、

認証用画面を前記画像形成装置のオペレーションパネルに表示させ、前記認証用画面から入力された認証データが認証条件を満たした場合に、前記画像形成装置の使用をするための画面を前記認証用画面に代えて前記オペレーションパネルに表示させる認証手順を実

行させるプログラムであって、前記システム側ソフトウェアとは別に前記画像形成装置に備えられることを特徴とするプログラム。

【請求項２２】

前記画像形成装置は、携帯端末と無線データ通信を行うための通信手段を更に有し、

前記プログラムは、前記通信手段により前記携帯端末から受信した認証用データを用いて前記認証手順を前記画像形成装置に実行させる請求項２１に記載のプログラム。

【請求項２３】

前記画像形成装置の利用に関するログ情報を収集する手順を前記画像形成装置に実行させる請求項２１に記載のプログラム。

【請求項２４】

前記利用に関するログ情報として印刷完了通知を収集し、印刷枚数が予め定めた許容枚数に達したときに前記オペレーションパネルに警告を表示させる手順を前記画像形成装置に実行させる請求項２３に記載のプログラム。

【請求項２５】

請求項２１ないし２４のうちいずれか１項に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【書類名】明細書
【発明の名称】画像形成装置、認証方法、及びプログラム
【技術分野】
【０００１】
本発明は画像形成装置に係り、特に、認証機能を備えた画像形成装置に関する。
【背景技術】
【０００２】
従来から、プリンタやコピー機等の画像形成装置に利用者制限モードを設け、使用時にユーザーコードを入れて認証することで、利用制限を解除する方式がある。また、プリンタ、コピー、ファクシミリ、スキャナなどの各装置の機能を１つの筐体内に収納した画像形成装置にも利用者制限モードが設けられている。
【０００３】
また、上記の画像形成装置にキーカード、プリペイドカード、コインラックやカードリーダーなどの装置を接続し、カードのセットやコインの投入により、利用制限解除や課金管理を可能とする方式も普及している。
【特許文献１】特開２００２－１４９３６２号公報
【特許文献２】特開２００２－１０８５８３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
上記の利用制限等の目的は、画像形成装置が使用される組織や企業等のユーザーにより様々であり、各ユーザーの目的に応じた方法で利用制限や課金管理を行う手段を実装した画像形成装置を迅速に提供することが要望されている。
しかしながら、従来の技術における利用制限のための認証は、画像形成装置に固定的に備えられるシステムソフトウェアに認証機能を含めることによって実現していたので、各ユーザーの希望に応じて認証機能をカスタマイズすることを迅速に行うことはできなかった。
【０００５】
更に、利用制限や課金管理の目的によっては、その方法を変更しなければならない場合があり、利用制限や課金管理の方法を容易に変更できることが要望されている。しかし、従来のようにシステムソフトウェアに利用制限のための認証機能を組み込む方式では、システムにおける一部の機能のみを変更することは、変更をする予定のない他の機能に与える影響も大きいことから、容易ではなかった。
【０００６】
本発明は、上記の点に鑑みてなされたものであり、種々の目的に応じた認証機能を容易に追加、変更することを可能とする画像形成装置、認証方法及びプログラムを提供することを目的とする。
【課題を解決するための手段】
【０００７】
上記の目的は、以下の発明の構成により達成できる。
【０００８】
請求項１に記載の発明は、アプリケーションと、当該アプリケーションにシステム側サービスを提供するシステム側ソフトウェアとを有する画像形成装置であって、認証用画面を前記画像形成装置のオペレーションパネルに表示させ、前記認証用画面から入力された認証用データが認証条件を満たした場合に、画像形成装置の使用をするための画面を前記認証用画面に代えて前記オペレーションパネルに表示させる認証モジュールを有し、当該認証モジュールは、前記システム側ソフトウェアとは別に備えられていることを特徴とする画像形成装置である。
【０００９】
本発明によれば、認証条件を満たさない限り認証用画面から画像形成装置の使用画面に

移行させないようにでき、利用制限をかけることができる。これにより、認証用画面及び認証条件を適宜設定すれば、種々の目的に応じた利用制限が可能となる。また、ＲＯＭ等に固定的に備えられるシステム側ソフトウェアとは別に認証モジュールを設けたため、認証モジュールを容易に追加、変更することが可能となる。

【００１０】

請求項２に記載の発明は、請求項１に記載の画像形成装置において、前記システム側ソフトウェアは認証機能部を含み、利用者により前記画像形成装置における特定のアプリケーションが選択されたときに、前記画像形成装置は、アプリケーションの種類と、前記認証モジュール又は前記システム側ソフトウェアの認証機能部との対応付けを示す情報を参照することにより、前記特定のアプリケーションに対応する前記認証モジュール又は前記システム側ソフトウェアの認証機能部を用いて認証を行うものである。

【００１１】

本発明によれば、システム側ソフトウェアの認証機能と、追加的に搭載される認証モジュールとを、アプリケーション毎に選択的に使用することが可能となる。

【００１２】

請求項３に記載の発明は、請求項１又は２に記載の画像形成装置において、前記認証モジュールを前記画像形成装置に外付けされる記録媒体から実行する手段、又は前記認証モジュールを前記記録媒体から前記画像形成装置にロードして実行する手段を有するものである。

【００１３】

本発明によれば、カスタマイズした認証モジュールを必要に応じて実行させることが可能となる。

【００１４】

請求項４に記載の発明は、請求項１又は２に記載の画像形成装置において、前記認証モジュールを、前記画像形成装置と通信ネットワークを介して接続されたサーバからダウンロードし、実行する認証モジュール実行手段を有する。また、請求項５に記載の発明は、請求項４に記載の画像形成装置において、前記認証モジュールは、Ｊａｖａ（登録商標）プログラムであり、前記認証モジュール実行手段は、クラスライブラリと仮想マシンを含む。このような構成によれば、認証モジュールの追加変更を一層容易に行うことが可能となる。

【００１５】

請求項６に記載の発明は、請求項１又は２に記載の画像形成装置において、前記画像形成装置は、携帯端末と無線データ通信を行うための通信手段を更に有し、前記認証モジュールは、前記通信手段により前記携帯端末から受信した認証用データを用いて認証を行う。また、請求項７に記載の発明は、請求項６に記載の画像形成装置において、前記画像形成装置は、前記携帯端末から前記認証用データを入力させるための画面データを生成し、当該画面データを前記携帯端末に送信する手段を有するというものである。

【００１６】

本発明によれば、オペレーションパネルのみならず、ＰＤＡ、携帯電話等の携帯端末から認証用データを入力することができる。

【００１７】

請求項８に記載の発明は、請求項１ないし７のうちいずれか１項に記載の画像形成装置において、前記認証用データとして、部署名又はアプリケーションの使用目的を利用者に入力させるものである。これにより、種々の目的に応じた認証を行うことが可能となる。

【００１８】

請求項９に記載の発明は、請求項１又は２に記載の画像形成装置において、前記認証モジュールの認証用画面を、前記画像形成装置の立ち上がり時に優先的に前記オペレーションパネルに表示させる手段を有するものである。本発明によれば、電源を投入してすぐに認証画面を表示させ、利用制限を行うことが可能となる。

【００１９】

請求項１０に記載の発明は、請求項１又は２に記載の画像形成装置において、前記オペレーションパネルに前記認証用画面以外の画面を表示しているときに、前記画像形成装置におけるジョブの終了、又は前記画像形成装置のシステムオートクリア、又は前記認証モジュールを使用するためのキー入力がなされた場合に、前記認証用画面以外の画面に代えて前記認証用画面を表示させる手段を有するものである。

【００２０】

本発明によれば、画像形成装置の使用中にその場から離れた後にジョブが終了しても、自動的に認証用画面を表示させることができる。また、画像形成装置を放置していた場合等に、システムオートクリア機能が作動した場合にも、認証用画面を表示させることができる。また、画像形成装置の使用中に認証モジュールを使用するためのキー入力をしておけば、認証用画面を表示させることができる。これらにより、他人による不正使用を防止することが可能となる。

【００２１】

請求項１１に記載の発明は、請求項１０に記載の画像形成装置において、前記画像形成装置は、所定のジョブが終了した後、一定時間の経過を検出した場合に前記システムオートクリアを起動し、前記認証用画面を表示するというものである。

【００２２】

請求項１２に記載の発明は、請求項１又は２に記載の画像形成装置において、前記認証モジュールは、前記画像形成装置の利用に関するログ情報を収集する手段を有するというものである。

【００２３】

また、請求項１３に記載の発明は、請求項１２に記載の画像形成装置において、前記認証モジュールは、前記利用に関するログ情報として印刷完了通知を収集し、印刷枚数が予め定めた許容枚数に達したときに前記オペレーションパネルに警告表示をさせるものである。

【００２４】

請求項１４～請求項１９に記載の発明は、上記画像形成装置における認証方法の発明である。請求項２０～請求項２４に記載の発明は、上記画像形成装置の認証モジュールに対応するプログラムである。請求項２５に記載の発明は、上記プログラムを記録した記録媒体の発明である。

【発明の効果】

【００２５】

本発明によれば、ＲＯＭ等に固定的に備えられるシステム側ソフトウェアとは別に認証モジュールを設けたため、容易に追加、変更可能な認証機能を備えた画像形成装置を提供できる。

【発明を実施するための最良の形態】

【００２６】

（第１の実施の形態）

まず、本発明の第１の実施の形態の概要について、図１、２を用いて説明する。

【００２７】

本実施の形態における画像形成装置（以下、複合機という）は、表示部、印刷部及び撮像部などの画像形成処理で使用されるハードウェア資源を備えるとともに、プリンタ、コピー又はファクシミリなどのアプリケーションを複数搭載している。また、これらのアプリケーションとハードウェア資源との間に介在してハードウェア資源の管理、実行制御並びに画像形成処理を行う各種コントロールサービスを備えている。この複合機は、アプリケーションを追加することが従来の複合機に比べて容易にできるので、ユーザーのニーズに応じたアプリケーションを開発し、既にユーザーサイドで稼動している複合機に必要に応じて新規アプリケーションを追加することが可能である。なお、コントロールサービスはシステム側ソフトウェアと称することができる。

【００２８】

この複合機では、各アプリケーションに対して、図１に示すような共通の操作部（以下、オペレーションパネルという）を使用する。アプリケーション切り替えは、オペレーションパネルにおけるアプリケーション切り替えキーを押下しすることで行うことができる。

本実施の形態における複合機は、本発明に係る認証モジュールを備える。認証モジュールは、システム側に固定的に備えられている認証機能とは別に設けられているものである。この認証モジュールによる画面がオペレーションパネルに表示されている場合、認証条件をクリアしない限り、画面を他のアプリケーション等に切り替えることができない。なお、認証モジュールが使用する認証のための情報は複合機内に備えていてもよいし、認証情報を外部の認証・課金サーバに置き、当該認証・課金サーバにネットワークを介して認証を依頼するような構成としてもよい。

【００２９】

また、本実施の形態における複合機では、認証モジュールを“優先アプリ”に設定することができる。優先アプリとは、電源ＯＮ時又はシステムリセット時に画面の制御権を持って立ち上がるアプリケーションである。優先アプリは、複合機が立ち上がった際にオペレーションパネルの画面制御権を持っている。従って、認証モジュールを“優先アプリ”に設定することで、認証条件をクリアしない限り、所望のアプリケーションの利用が制限される。なお、“優先アプリ”として設定できるものは、いわゆるアプリケーションに限られず、システム側のソフトウェアでもよい。すなわち、本明細書における“優先アプリ”は、アプリケーション及びシステム側のソフトウェアを含む意味で使用する。

【００３０】

認証・課金サーバを用いる場合の全体の構成例を図２に示す。図２は、複合機１００と認証・課金サーバ１５０とがネットワークを介して接続される構成を示している。

【００３１】

図２に示す構成における複合機の動作の概要を次に説明する。

【００３２】

認証モジュールが優先アプリとして立ち上がると、オペレーションパネルの画面には認証を行うため「ユーザーコード」及び「パスワード」の入力画面を表示する。また、複合機に備えられたカードリーダーを用いてカードから情報を取得する場合には、「カードを通してください」等の表示を行う。

【００３３】

ユーザーコードを用いる例について説明すると、まず複合機１００を使用したいユーザーは、ユーザーコードをオペレーションパネルの画面から入力する。複合機１００はユーザーコードの入力を受け、ネットワーク上に有る認証・課金サーバ１５０に問い合わせを行う。認証・課金サーバ１５０側では、入力されたユーザーコードに一致するデータが有れば、認証ＯＫの通知を認証モジュールに返答する。認証モジュールは、オペレーションパネルに、「利用したいアプリのキーを選択下さい」等と表示し、アプリ切り替えキーを有効にする。

【００３４】

ここでユーザーがコピーキーを押下しすると、コピーの画面が表示され、原稿をセットしてコピーを開始できる。コピーが完了し、一定時間（タイマー設定：例えばアイドル状態３０秒）経過し、システムオートクリアが起動されると、認証モジュールの画面を表示して利用制限モードに戻る。

【００３５】

次に、本発明の第１の実施の形態をより詳細に説明する。

【００３６】

図３は、本実施の形態における複合機の構成を示すブロック図である。図３に示すように、複合機１００は、白黒ラインプリンタ（B&W LP）１０１と、カラーラインプリンタ（Color LP）１０２と、スキャナ、ファクシミリなどのハードウェアリソース１０３などを有するとともに、プラットホーム１２０とアプリケーション１３０とから構成されるソフ

トウェア群１１０と、電源投入時に実行される複合機起動部１４０とを備えている。

【００３７】

複合機起動部１４０は、複合機１００の電源投入時にまずはじめに実行され、機器の初期化、診断を行い、各コントロールサービス、各アプリケーション等を起動するものである。

プラットホーム１２０は、アプリケーション１３０からの処理要求を解釈してハードウェア資源の獲得要求を発生させるコントロールサービスと、一又は複数のハードウェア資源の管理を行い、コントロールサービスからの獲得要求を調停するシステムリソースマネージャ（ＳＲＭ）１２３と、汎用ＯＳ１２１とを有する。

【００３８】

コントロールサービスは、複数のサービスモジュールから形成され、ＳＣＳ（システムコントロールサービス）１２２と、ＥＣＳ（エンジンコントロールサービス）１２４と、ＭＣＳ（メモリコントロールサービス）１２５と、ＯＣＳ（オペレーションパネルコントロールサービス）１２６と、ＦＣＳ（ファックスコントロールサービス）１２７と、ＮＣＳ（ネットワークコントロールサービス）１２８とから構成される。なお、このプラットホーム１２０は、あらかじめ定義された関数により前記アプリケーション１３０から処理要求を受信可能とするアプリケーションプログラムインタフェース（ＡＰＩ）を有する。

【００３９】

汎用ＯＳ１２１は、ＵＮＩＸ（登録商標）などの汎用オペレーティングシステムである。　ＳＲＭ１２３のプロセスは、ＳＣＳ１２２とともにシステムの制御及びリソースの管理を行うものである。ＳＣＳ１２２のプロセスは、アプリ管理、操作部制御、システム画面表示、ＬＥＤ表示、リソース管理、割り込みアプリ制御等を行い、ＥＣＳ１２４のプロセスは、ハードウェアリソース１０３のエンジンの制御を行う。なお、ＳＣＳ１２２は、上記の管理機能に加えて、ユーザー認証の機能を含むものである。例えば、ユーザーから入力されたユーザコードとパスワードが、予め登録してあるユーザコードとパスワードに一致したときに複合機の使用を許可するといった機能を有している。

【００４０】

ＭＣＳ１２５のプロセスは、画像メモリ、ハードディスク装置（ＨＤＤ）の利用に関する処理を行う。また、ＦＣＳ１２７のプロセスは、ファクシミリ送受信のための処理等を行う。ＮＣＳ１２８は、ネットワークＩ／Ｏを必要とするアプリケーションに対して共通に利用できるサービスを提供するためのプロセスである。すなわち、ＮＣＳ１２８は、データ通信のためのプロトコル処理等を行う機能を含むものである。

【００４１】

ＯＣＳ１２６のプロセスは、オペレータ（ユーザー）と本体制御間の情報伝達手段となるオペレーションパネル（操作パネル）の制御を行う。ＯＣＳ１２６は、オペレーションパネルからキー押下をキーイベントとして取得し、取得したキーに対応したキーイベント関数をＳＣＳ１２２に送信するＯＣＳプロセスの部分と、アプリケーション１３０又はコントロールサービスからの要求によりオペレーションパネルに各種画面を描画出力する描画関数やその他オペレーションパネルに対する制御を行う関数などがあらかじめ登録されたＯＣＳライブラリの部分とから構成される。

【００４２】

アプリケーション１３０は、プリンタ用のアプリケーションであるプリンタアプリ１１１と、コピー用アプリケーションであるコピーアプリ１１２と、ファクシミリ用アプリケーションであるファックスアプリ１１３と、スキャナ用アプリケーションであるスキャナアプリ１１４を有する。更に、必要に応じて複合機に追加される追加アプリ１１５、１１６を有している。これらの追加アプリは、フラッシュカード、ＳＤカード等から必要に応じてインストール（ロード）できる。また、フラッシュカード、ＳＤカード等から起動することも可能である。更に、ネットワークを介して他のサーバからインストール、及び起動することも可能である。

【００４３】

更に、複合機１００は、本発明に係る認証モジュール１１７を有している。認証モジュール１１７は、上記の追加アプリケーションと同様に、フラッシュカード、ＳＤカード、ネットワーク接続されたサーバ等から容易に複合機に追加することが可能である。また、認証モジュールの機能変更をした場合には、容易に新しい認証モジュールをインストールすることが可能である。認証モジュールは、図３に示すように、コントロールサービス側に備えてもよいし、図４に示すようにアプリケーションとして備えてもよい。

【００４４】

アプリケーション１３０の各プロセス、コントロールサービスの各プロセスは、関数呼び出しとその戻り値送信及びメッセージの送受信によってプロセス間通信を行いながら、その処理を実行している。そして、コントロールサービスがアプリケーション１３０に対し共通サービスを提供している。なお、コントロールサービスはシステム側ソフトウェアと称する場合がある。また、コントロールサービスによりアプリケーションに対して提供されるサービスをシステム側サービスと称する場合がある。

【００４５】

図５は、図３、４に示した複合機１００のハードウェア構成図である。図５に示すように、この複合機１００は、コントローラボード２００と、オペレーションパネル２１０と、ファックスコントロールユニット（ＦＣＵ）２２０と、ＵＳＢデバイス２３０と、ＩＥＥＥ１３９４デバイス２４０と、ブルートゥースデバイス２５０と、エンジン部２６０から構成されている。

【００４６】

コントローラボード２００は、ＡＳＩＣ２０１、ＣＰＵ２０２、ＲＡＭ２０３、ＲＯＭ２０４、ＨＤＤ２０５、フラッシュカードインタフェース部２０６、ネットワークインターフェースコントローラ２０９から構成されている。

【００４７】

オペレーションパネル２１０は、ＡＳＩＣ２０１に直接接続されている。ＦＣＵ２２０、ＵＳＢデバイス２３０、ＩＥＥＥ１３９４デバイス２４０、ブルートゥースデバイス２５０及びエンジン部２６０は、ＰＣＩバスを介してＡＳＩＣ２０１に接続されている。

【００４８】

ネットワークインターフェースコントローラ２０９は、ネットワーク２７１に接続されている他の機器とＭＡＣアドレスなどを用いて通信する。ＦＣＵ２２０は電話網２７２に接続されている。また、ＵＳＢデバイス２３０、ＩＥＥＥ１３９４デバイス２４０及びブルートゥースデバイス２５０により、他の端末２７３～２７５に接続することができる。他の端末２７３～２７５としては、ＰＣの他、ＰＤＡ、携帯電話等でもよい。フラッシュカードインタフェース部２０６は、挿入されたフラッシュカード２０７とデータのやりとりを行うインタフェースである。更に、ＳＤカードインタフェース部を備えてもよい。

【００４９】

ＲＯＭ２０４には、上述の各アプリケーション、プラットホーム１２０を構成する各コントロールサービス及びＳＲＭ１２３の各プログラムが格納されている。

【００５０】

本実施の形態では、認証モジュール１１７は、フラッシュカード２０７から直接起動するが、フラッシュカード２０７からＨＤＤ２０５にインストールして起動してもよい。プリンタアプリ１１１、コピーアプリ１１２、ファックスアプリ１１３、スキャナアプリ１１４などのアプリケーション１３０、各コントロールサービスは出荷時にＲＯＭ２０４に組み込まれている。これらのアプリケーションやコントロールサービスは、複合機１００の起動時（電源投入時）に複合機起動部１４０によって起動される。すなわち、ＳＣＳ１２２が有する認証機能部は、出荷時にＲＯＭ２０４に組み込まれているので、その機能変更は容易でない。一方、認証モジュール１１７は、必要に応じてフラッシュカード、ＳＤカード等から起動できるので、追加、変更が容易である。

【００５１】

以下、本実施の形態における複合機１００の動作について詳細に説明する。

【００５２】
図６は、複合機１００の立ち上げ時の動作を示すフローチャートである。なお、この処理は、複合機起動部１４０により実行される処理である。
【００５３】
まず、電源投入もしくはリセット後、初期化処理が行われる（ステップＳ１）。初期化処理は、ＢＩＯＳ（Basic Input/Output System）及びブートローダ（Boot Loader）の起動、カーネル（Kernel）の起動、ハードウェアの初期化、診断等である。
【００５４】
次に、ＲＯＭ等のメモリ媒体におけるＲＯＭファイル（ｒｏｍｆｓ形式のファイル）をサーチし（ステップＳ２）、メモリ媒体の所定位置に配置されたアプリ設定ファイルをサーチする（ステップＳ３）。例えば、図７に示すように、ＲＯＭとフラッシュカードにＲＯＭファイル（ＲＯＭ０とＲＯＭ１）があり、それぞれの先頭部分にアプリ設定ファイルが存在する。ＲＯＭの中のアプリ設定ファイルの例を図８（ａ）に示し、フラッシュカードの中のアプリ設定ファイルの例を図８（ｂ）に示す。なお、図８中、“－２”等は起動優先度を示している。
【００５５】
次に、ＲＯＭの中のアプリ設定ファイルを参照して、mount命令に従ってＲＯＭファイルシステム（ｒｏｍｆｓ）をマウントし、マウント先のアプリ設定ファイル（図８（ｂ））も参照して、アプリケーションの起動条件、順序をチェックし（ステップＳ４）、各種アプリケーション、ＳＣＳを含むコントロールサービスを起動する（ステップＳ５）。図７、８の例では、Ａ→Ｃ→Ｂ→Ｄ→Ｅの順にアプリケーションが起動される。
【００５６】
ハードディスク（ＨＤＤ２０５）にもアプリケーションが置かれている場合には、ハードディスクのプログラムを起動するためのランチャーを起動する。ランチャーは、ハードディスクを起動後、ハードディスクの準備が完了するまで待ち（ステップＳ６）、その後、ＲＯＭファイル及びアプリ設定ファイルのサーチを行い、アプリ設定ファイルに従って、アプリケーションの起動を行う（ステップＳ７～Ｓ９）。
【００５７】
図９は、コントロールサービスの１つであるＳＣＳ１２２の起動後の複合機１００の動作を示すフローチャートである。
【００５８】
アプリ設定ファイルに従ってＳＣＳプロセスが起動すると、まず、オペレーションパネル２１０にウィンドウが表示され（ステップＳ１１）、「お待ちください」等のメッセージが表示される。その間、起動した各アプリケーション（コピー、プリンタ等）のアプリ登録が行われる（ステップＳ１２）。ＳＣＳ１２２では、各アプリケーションからのアプリ登録依頼メッセージを受信して、ＲＡＭ等にアプリケーションの識別ＩＤ等を格納することによりアプリ登録を行う。
【００５９】
続いて、ＲＡＭ２０３等の記憶装置の所定の領域（以下、これを優先アプリ領域という）を参照することにより優先アプリの設定があるか否かをチェックする（ステップＳ１３）。記憶装置の優先アプリ領域に優先アプリの設定がなければ、デフォルトのアプリケーション（通常はコピーアプリ）が優先アプリとして設定され（ステップＳ１４）、認証モジュールが優先アプリとして設定されていれば認証モジュールが優先アプリとなる（ステップＳ１５）。
【００６０】
あるアプリケーションを優先アプリ領域に優先アプリとして設定することは、そのアプリケーションに、オペレーションパネルへのアクセス権限を付与することを意味する。すなわち、画面制御権限を付与することを意味する。以下、認証モジュール１１７が優先アプリとして設定されている場合について説明する。認証モジュール１１７が優先アプリとして設定されると、ＳＣＳ１２２は、認証モジュール１１７に対して画面制御権限付与の

通知メッセージを送信する（ステップＳ１６）。

【００６１】

認証モジュール１１７は、ＳＣＳ１２２から画面制御権限付与のメッセージを受信すると、オペレーションパネル２１０に対してユーザー認証用の画面を表示する（ステップＳ１７）。より詳細には、オペレーションパネル２１０に対する画面表示は、認証モジュール１１７の表示依頼によりＯＣＳ１２６が行う。すなわち、認証モジュール１１７がＯＣＳ１２６に対して表示すべき描画情報を指定して描画関数の呼び出しを行うことにより、ＯＣＳ１２６が指定された描画情報の表示処理を行う。

【００６２】

ユーザー認証用の画面に対するユーザーからの入力が認証条件を満たせば（ステップＳ１８のＹ）、機器利用許可のメッセージとともに、アプリケーションを選択してくださいとのメッセージがオペレーションパネルに表示される（ステップＳ１９）。なお、オペレーションパネル２１０からのキー入力、ボタン押下などの操作は、ＯＣＳ１２６とＳＣＳ１２２を介して認証モジュールに通知されるものである。

【００６３】

ユーザーがオペレーションパネル２１０からアプリケーションを選択すると、選択されたアプリケーションはＳＣＳ１２２に通知され、ＳＣＳ１２２は、優先アプリの設定内容を選択されたアプリケーションに変更する。そして、その選択されたアプリケーションに対して画面制御権限付与のメッセージを通知する。その後、選択されたアプリケーションの実行、処理が行われる（ステップＳ２０）。

【００６４】

アプリケーションの実行中においては、システムオートクリア、認証モジュールキー押下し、アプリケーションのジョブ終了のときなどに、認証モジュールに画面の制御権限が移行し、認証モジュールは認証画面を表示する。

【００６５】

上記の例では、最初に優先アプリとして認証モジュール１１７が設定されているが、その設定は次のようにして行う。複合機１００の初期設定画面から優先アプリ設定を選択し、図１０に示すような、追加アプリ（認証モジュール等）を含む優先アプリ設定画面を表示させる。そして、その画面から所望の追加アプリを選択する。これにより、選択された追加アプリ名が優先アプリ領域に登録される。複合機起動時には、この情報をＳＣＳ１２２が参照することにより、優先アプリ設定の有無を判断し、複合機１００の立ち上がり時に、認証モジュールに認証画面を表示させることが可能となる。

【００６６】

図１１は、認証モジュール１１７を用いた場合における、オペレーションパネル２１０の画面状態遷移図である。なお、図１１は、コピーアプリに着目した図である。

【００６７】

同図に示すように、電源ＯＮ又はリスタートにより、まず認証モジュール画面に遷移し、認証条件入力待ちになる（状態１）。ユーザーからの入力が認証条件を満たさなければ、認証モジュール画面のままである。ユーザーからの入力が認証条件を満たす場合（認証ＯＫの場合）には、アプリ選択画面を表示してアプリ切替キーイベント待ちになり（状態２）、選択するアプリケーションの入力を受けて、当該アプリケーションの画面に移行する。

【００６８】

例えば、コピーアプリを選択した場合、コピー用の画面が表示され、コピー可能になる（状態３）。そして、コピーアプリ動作中において、ジョブ終了、システムオートクリア、認証モジュールに遷移するためのキーイベント等により認証モジュール画面に戻る。

【００６９】

次に、図１２のフローチャートを参照して認証モジュール１１７の動作を説明する。図１２の左側には、各動作に対応したオペレーションパネル２１０の表示内容を示している。オペレーションパネルへの表示及びオペレーションパネルからのデータ入力はＯＣＳ１

２６を介して行われるが、図１２ではＳＣＳ１２２、認証モジュール１１７、コピーアプリ１１２に着目し、ＯＣＳ１２６を図示していない。

【００７０】

同図中、最初は認証モジュール画面が表示されており、認証条件入力待ちの状態となっている（認証条件入力待ち期間Ｐ１）。この状態では、仮にアプリ切替キーイベントがＳＣＳ１２２に通知され、ＳＣＳ１２２から認証モジュール１１７に対して画面解放要求が出されても、認証モジュール１１７はそれを受け付けず、ＳＣＳ１２２に対してＮＧを返す。すなわち、認証条件入力待ち期間Ｐ１では、認証モジュール１１７は、認証条件を満たす入力がない限り画面解放要求に対してＮＧを返し、画面解放を許可しない。

【００７１】

オペレーションパネル２１０からユーザーコードやパスワード等の認証情報が入力されると、ＳＣＳ１２２はその認証情報を認証モジュール１１７に通知し、認証情報が正当かどうかのチェックを行い、認証Ｏ.Ｋであれば、その旨をＳＣＳ１２２に通知する（認証チェック）。

【００７２】

認証済み期間Ｐ２において、認証モジュール１１７はアプリ切替画面表示を行う。なお、アプリ切替画面表示はＳＣＳ１２２が行ってもよい。そして、アプリ切替画面表示中に、コピーアプリ１１２が選択されると、コピーアプリ切替キーイベントがＳＣＳ１２２に通知され、ＳＣＳ１２２から画面解放要求が認証モジュール１１７に送られる。認証済みであるので、認証モジュール１１７は、画面解放ＯＫをＳＣＳ１２２に対して通知する。

【００７３】

そして、ＳＣＳ１２２は優先アプリ領域にコピーアプリを設定し、画面制御権限付与の通知メッセージをコピーアプリに通知する。そして、コピーアプリ１１２は、コピー画面を表示する。

【００７４】

その後、コピー使用期間Ｐ３において、コピーアプリが使用される。ここで、コピー中にオペレーションパネル２１０から所定のキーを押すなどして認証モジュール１１７が選択されると、認証モジュールキーイベントがＳＣＳ１２２に通知される。そして、ＳＣＳ１２２はコピーアプリに対して画面解放要求を出すと、コピーアプリはＳＣＳ１２２に画面解放ＯＫを通知する。そして、ＳＣＳ１２２は、優先アプリ領域の設定を認証モジュール１１７にし、画面制御権限付与のメッセージを認証モジュール１１７に対して通知する。そして、認証モジュール１１７は認証モジュール画面を表示し、認証条件入力待ちとなる（認証条件入力待ち期間Ｐ４）。なお、コピー中に認証モジュール画面を表示させることを可能としたことにより、コピー中にその場を離れた場合でも、他人に無断でコピーをとられてしまうといったことを防止できる。

【００７５】

コピー中に認証モジュールキーイベントを発生させない場合に、コピー終了後複合機１００をしばらく放置しておくと、ＳＣＳ１２２によりシステムオートクリアが作動し、ＳＣＳ１２２が認証モジュール１１７に制御権限を移行させ、認証モジュール１１７は認証モジュール画面を表示し、認証条件入力待ち期間Ｐ５に入る。

【００７６】

なお、コピー完了後に、認証モジュール１１７による利用制限の代わりに、ＳＣＳ１２２による利用制限機能を動作させ、「カードを通して下さい」といった警告用のポップアップウインドウを開いて利用を制限してもよい。

【００７７】

上記のように、第１の実施の形態によれば、認証モジュール１１７により複合機１００全体の利用制限をかけることができる。上記の例では、認証条件をユーザーコード等の合致としたが、その他、用途、要求に応じた認証条件を用い、その認証条件にあった認証画面を表示することが可能である。例えば、企業独自の社員カード、指紋等による認証を行うことができる。認証方法自体も特に限定されることはなく、例えば、複合機１００自身

が認証条件をチェックする方法や遠隔の認証・課金サーバが認証条件をチェックする方法の何れの方法もとることができる。また、認証条件や認証方法を変更する場合には、認証モジュールを変更すればよく、他のアプリケーション（コピー、プリンタ、ＦＡＸ等）やシステム側ソフトウェアを変更する必要がないため、容易にカスタマイズができる。

【００７８】

また、コピー中に認証モジュール画面に画面遷移することができるので、大量のコピーをセットしてその場を立ち去っても、再び認証を行わない限り、他のアプリケーション画面へ移れない。従って、他人に不正に使用されてしまう恐れがなくなる。また、認証用のアプリケーション画面に移行させることを忘れて、複合機１００の前から離れても、コピー完了後にシステムオートクリアが働いて認証画面を表示させることが可能なので、他人に不正に使用されてしまう恐れがなくなる。

【００７９】

（第２の実施の形態）

次に、本発明の第２の実施の形態について説明する。第２の実施の形態は、コピーの枚数管理を行う場合において認証モジュール１１７が残度数のカウントを行う形態である。すなわち、認証モジュール１１７が、認証のみでなく、課金に関する処理も行う形態である。

【００８０】

図１３に、第２の実施の形態における画面遷移を示す。同図に示すように、第２の実施の形態では、コピーアプリ使用中（状態３）に、コピー枚数が許容枚数をオーバーした場合に、認証モジュール１１７が警告メッセージを表示する（状態４）。この場合、残度数の更新を行えばコピー画面に戻るが、更新されなければ印刷中止となり認証モジュール画面に戻る。

【００８１】

図１４の構成図及び図１５に示すシーケンスチャートを用いて、第２の実施の形態における複合機１００の処理の流れを説明する。なお、図１４に示す構成は、複合機１００に認証・課金サーバ１５０がネットワークを介して接続される構成である。

【００８２】

認証モジュール画面にてユーザーコード等を入力した後、認証・課金サーバ１５０が、登録されたユーザーコードと入力されたユーザーコードとを比較することによりユーザー認証を行う。そして、認証が成功した場合に、認証されたユーザーのコピー利用可能枚数（残度数という）が複合機１００に送られる（ステップＳ１０１）。

【００８３】

認証モジュール１１７はＮＣＳ１２８を介してその残度数を受信し、それを不揮発性ＲＡＭ、ＨＤＤ等の記憶装置に保存する（ステップＳ１０２）。なお、この残度数は、ユーザー毎に課金する場合にはユーザー単位であり、記憶装置には、ユーザー毎の残度数を記録する。また、例えば部門毎に課金する場合は部門単位に残度数を記録する。

【００８４】

認証が成功したことにより、第１の実施の形態で説明したようにオペレーションパネルにアプリ選択指示が表示され、そこでコピーアプリを選択することによりコピーアプリ１１２に画面制御権限が移行し、コピー画面が表示される。

【００８５】

コピーアプリ１１２は、認証モジュール１１７に残度数が０より大きいか否かを問い合わせ、認証モジュール１１７は、０より大きい場合に印刷ＯＫを返す（ステップＳ１０３）。なお、問い合わせはＳＣＳ１２２を介して行うこともできる。また、コピーアプリ１１２は、残度数の値を記憶装置をチェックすることにより確認してもよい。

【００８６】

ユーザーによりコピーが開始されると、コピーアプリ１１２は、印刷ジョブをＥＣＳ１２４に通知する（ステップＳ１０４）。ジョブに応じたＥＣＳ１２４からの命令を受けたコピーエンジン側からは、１枚印刷するたびに、ＥＣＳ１２４に対して、印刷完了のイベ

ント通知をし（ステップＳ１０５）、そのイベントはＳＣＳ１２２経由で認証モジュール１１７に通知される（ステップＳ１０６）。

【００８７】

認証モジュール１１７は、残度数から印刷枚数を減算して残度数を更新する（ステップＳ１０７）。そして、認証モジュール１１７は、ページ単位又は定期的にＮＣＳ１２８経由で認証・課金サーバ１５０に残度数を通知する（ステップＳ１０８）。

【００８８】

残度数が０になると、認証モジュール１１７からコピーアプリ１１２に対して印刷中止の通知をする（ステップＳ１０９）。なお、この通知はＳＣＳ１２２経由で行うこともできる。その後、コピーアプリはコピージョブをキャンセルして、ＥＣＳ１２４に対して印刷中止を通知する（ステップＳ１１０）。そして、認証モジュール１１７は、残度数がない旨の警告表示をオペレーションパネルに対して行う。

【００８９】

認証・課金サーバ１５０側で残度数更新がなされると、新たな残度数が認証モジュール１１７に通知され（ステップＳ１１１）、認証モジュール１１７からコピーアプリ１１２に対して残度数更新の通知がされ（ステップＳ１１２）、コピーアプリ１１２は、ＥＣＳ１２４に対してコピー再開要求をする（ステップＳ１１３）。そして、コピーが再開される。

【００９０】

なお、利用中に残度数が０になった場合に、コピー動作を停止する処理をＳＣＳ１２２が行うことも可能である。この場合、例えば、ＳＣＳ１２２が「キーカードを通してください」等のポップアップウインドウを表示することで、正しいキーカードを通さない限り、アプリケーションの利用を制限することができる。

【００９１】

また、上記の例では認証モジュール１１７が印刷完了通知を収集することにより、残度数管理を行っているが、これ以外にも、所望のアプリケーションを使用するときに発生する一連の操作や印刷、読みとり、ＦＡＸ送信などに関する情報をユーザーのＩＤに関連づけて収集するように構成することが可能である。これにより、誰がいつ何をどの位使用したかのログ情報を管理することが可能となり、そのログ情報に応じて、課金することも可能である。

【００９２】

上記のように、第２の実施の形態によれば、認証モジュール１１７が、印刷完了通知等のログ情報を収集する。ここで、認証モジュール１１７は、ＳＣＳ１２２等のコントロールサービスと異なり、後から追加可能なモジュールであるため、ログ情報の収集方法を変更することが容易であり、市場の要求に応じた課金や利用状況の把握を行うことが可能となる。例えば、紙サイズ、各種印刷条件（両面印刷、集約印刷、ステープル有無等）、印刷枚数、ジャム発生回数等の情報をユーザー毎あるいは部門毎に収集することにより、複合機１００の利用状況を把握できる。また、誰がどんな文書を何の目的でコピーしたか、ＦＡＸしたか、あるいはスキャンしたかなどの情報を入力させ、収集することにより、より具体的に複合機１００の利用状況を管理することが可能となる。これらの情報は、認証画面でユーザーコードやパスワードに加えて、それらの情報も入力しないと利用が許可されないように画面を設計することで、容易に収集することができる。

【００９３】

[認証モジュールの構成]

図１６に、第１、第２の実施の形態において説明した認証モジュール１１７の構成の一例を示す。図１６に示すように、認証モジュール１１７は、認証制御部３０１、認証データ管理部３０２、利用制限管理部３０３、及び利用状況管理部３０４を有している。また、認証制御部３０１は、操作画面解放判定部３０１１とキー／イベント／タイマー監視部３０１２を含んでいる。

【００９４】

認証制御部３０１は、電源ＯＮ後の立ち上がり、システムリセット、又は印刷等のジョブ終了の後、認証モジュール１１７の認証画面を表示する機能を有している。また、認証制御部３０１は、認証画面から入力されたデータ（例えばユーザーコード）が、認証条件を満たすか否かの判定を行う。例えば、入力されたユーザーコードと予め登録されたユーザーコードとを比較し、両者が一致すれば認証成功と判定する。認証が成功しない限り、アプリケーションの使用は許可されない。操作画面解放判定部３０１１は、認証結果に応じて、認証画面を解除して、画面を他のアプリケーションのために解放してよいかどうかを判定する機能を有し、キー／イベント／タイマー監視部３０１２は、入力されるキー、イベント、及び、タイマーのタイムアウトを監視する機能を有する。

【００９５】

認証モジュール１１７の中のこの認証制御部３０１の部分を、ＩＣカード、ＳＤカード等の記憶媒体から、もしくはネットワークからのダウンロードにより、複合機１００に後から追加可能である。

【００９６】

認証データ管理部３０２は、ユーザコード、パスワード等の認証データの管理、及び、体系に沿った情報の管理を行なう。認証データ管理部３０２は、認証制御部３０１からの問い合わせに対し、必要なデータを取得し、認証制御部３０１に返す。また、認証データ管理部３０２が、入力されたデータが認証条件を満たすか否かの判定を行い、その判定結果を認証制御部３０１に返すようにしてもよい。更に、認証データ管理部３０２は認証データの更新／編集機能を有している。

【００９７】

利用制限管理部３０３は、認証とは別に、各ユーザー、グループ（組織）単位で、アプリケーション毎に利用制限を行なう機能を有している。例えば、ある部署にのみ特定のアプリケーションの使用を許可することを設定した場合、認証制御部３０１が表示する利用制限画面を介して入力された部署名をその設定内容と比較することにより、特定のアプリケーションの使用可否を決定する。更に、アプリケーション毎の利用制限に加え、各ユーザー、グループ（組織）単位で、特定のアプリケーションの使用量（例えばコピー枚数）の上限を設定する機能を有し、上限に到達すると、その旨を認証制御部３０１に通知する機能を有している。

【００９８】

利用状況管理部３０４は、認証されたユーザー、グループ毎に、アプリケーションの利用状況を管理する機能を有している。例えば、コピーであれば枚数を管理し、ネットワークを利用するアプリケーションであれば、データの送信先等のログを管理する。

【００９９】

なお、上記各管理部が管理するデータは、複合機１００のハードディスク等の格納されていてもよいし、ネットワーク接続された外部のサーバに格納されていてもよい。また、上記の各管理部を複合機１００内に備えることに代えて、ネットワーク接続された外部のサーバに備えてもよい。

【０１００】

[認証モジュールの他の構成例]

上記のとおり、本発明の認証モジュール１１７は、システム側に従来から設けられている認証機能（例えばＳＣＳ１２２の認証機能）に比べて、追加、変更を容易に行うことができる。すなわち、ユーザーの要望等に応じて変更した認証モジュール１１７を適宜複合機にインストールすることができる。

【０１０１】

また、認証モジュール１１７をＪａｖａ（登録商標）プログラムを用いて実装することにより、適宜外部のサーバからＪａｖａ（登録商標）プログラムを必要に応じてダウンロードしてすぐに実行することが可能となり、更に認証モジュール１１７の追加、変更が容易になる。

【０１０２】

Ｊａｖａ（登録商標）プログラムを用いた場合の認証モジュール１１７（Ｊａｖａ（登録商標）プログラム）を含むＪａｖａ（登録商標）実行環境１１８の構成例を図１７に示す。このＪａｖａ（登録商標）実行環境１１８は、図　３に示す複合機１００の構成におけるアプリケーション層に搭載される。

【０１０３】

図１７に示すように、このＪａｖａ（登録商標）実行環境１１８は、Ｊａｖａ（登録商標）プログラムである認証モジュール１１７、クラスライブラリ４０１、仮想マシン４０２、及びプログラムローダー４０３を有している。また、図１７には、Ｊａｖａ（登録商標）プログラムを提供するＷｅｂサーバ４００を示している。複合機１００とＷｅｂサーバ４００はネットワークにより接続されている。

【０１０４】

クラスライブラリ４０１は、Ｊａｖａ（登録商標）プログラムを実行するために必要なクラスライブラリと共に、複合機１００を操作するためのサービスを提供するクラスライブラリを含む。仮想マシン４０２は、Ｊａｖａ（登録商標）プログラムを解釈し、実行するためのものである。また、プログラムローダー４０３は、Ｗｅｂサーバ４００からのプログラムダウンロード、Ｊａｖａ（登録商標）プログラムの実行管理等を行うものである。このような環境において、開発されたＪａｖａ（登録商標）プログラムをＷｅｂサーバ４００にアップロードしておく。そして、プログラムローダー４０３がＷｅｂサーバ４００にアクセスし、ユーザ所望のＪａｖａ（登録商標）プログラムをダウンロードし、実行する。

【０１０５】

（第３の実施の形態）

次に、本発明の第３の実施の形態について説明する。第３の実施の形態では、システム側が固定的に有している認証機能（ＳＣＳ１２２等であり、以下、これをシステム側認証制御部と称する）と、本発明に係る認証モジュール１１７とを切り替えて用いる場合の例について説明する。以下、システム側認証制御部を使用して認証を行うモードを標準認証モードと呼び、本発明に係る認証モジュール１１７を使用して認証を行うモードを追加認証モードと呼ぶ。

【０１０６】

[システム側認証制御部による認証画面を利用する例]

まず、システム側認証制御部により表示される認証画面を利用して、システム側認証制御部もしくは認証モジュール１１７による認証を行う場合について説明する。

【０１０７】

本実施の形態では、システムの初期設定画面等により、アプリケーション毎に標準認証モードによる認証を行うか、もしくは追加認証モードによる認証を行うかの設定をする。図１８に、設定内容の例を示す。図１８に示す例では、コピーアプリ、追加アプリ２に標準認証モードが設定され、スキャナアプリ、追加アプリ１には追加認証モードが設定されている。なお、ＦＡＸアプリに対しては認証による利用制限をしない設定となっている。

【０１０８】

また、この例の場合、複合機１００の構成を模式的に表した図１９に示すように、追加認証モードのときに、システム側認証制御部５０１により表示される認証画面から入力されたデータが認証モジュール１１７に渡され、認証モジュール１１７による認証結果がシステム側認証制御部５０１に通知される。なお、システム側認証制御部５０１による認証画面は、図２０に示すようなユーザーにユーザコードとパスワードを入力させるための画面である。この認証画面を認証画面Ａと呼ぶ。

【０１０９】

次に、図２１に示すフローチャートを参照して、処理の流れを説明する。

【０１１０】

複合機の電源ＯＮの後（ステップＳ２０１）、オペレーションパネルにシステム側認証制御部５０１が認証画面Ａを表示する（ステップＳ２０２）。ユーザーは、オペレーショ

ンパネルのアプリ切り替えキーを押下げることにより、利用したいアプリケーションを選択する（ステップＳ２０３）。また、ユーザーは、システム側認証制御部５０１による認証画面からユーザーコードとパスワードを入力する（ステップＳ２０４）。システム側認証制御部５０１はこれらのキー情報を取得する。

【０１１１】

システム側認証制御部５０１は、選択されたアプリケーションに対する認証モードを、図１８に示す設定内容から確認し（ステップＳ２０５）、標準認証モードであれば、複合機１００のシステム側で管理されている予め登録されたデータと、入力されたデータとを比較することによりシステム側認証制御部５０１が認証を行う（ステップＳ２０６）。認証成功であれば、認証画面Ａに代えて、選択されたアプリケーションの画面が表示される（ステップＳ２０７）。

【０１１２】

認証モードの設定内容が追加認証モードである場合は、システム側認証制御部５０１は、認証モジュール１１７にユーザーコードとパスワードを渡す（ステップＳ２０８）。

【０１１３】

認証モジュール１１７では、システム側認証制御部５０１から渡されたユーザーコードとパスワードを基に、認証モジュール１１７が管理している認証データや利用制限データを参照して認証を行い（ステップＳ２０９）、当該アプリケーションが当該ユーザーにより利用可能であれば、システム側認証制御部５０１に対して利用可能通知を返す（ステップＳ２１０）。なお、認証モジュール１１７が、外部のサーバへユーザーコードとパスワードを送信することにより問い合わせを行う場合には、当該サーバからの結果を待って、システム側認証制御部５０１への通知を行う。認証成功の通知を受けたシステム側認証制御部５０１は、最初に表示していた認証画面Ａに代えて、アプリケーションの画面の表示を許可し、アプリケーションの画面が表示される（ステップＳ２１１）。

【０１１４】

[システム側認証制御部による認証画面と認証モジュールによる認証画面を利用する例]

次に、システム側認証制御部５０１による認証画面Ａと認証モジュール１１７による認証画面の両方を利用する場合について説明する。この例における認証モードの設定内容は上記と同様に図１８に示す通りである。

【０１１５】

この例の場合、図２２に示す通り、設定内容に応じて、追加認証モードに設定されているアプリケーションに対しては認証モジュール１１７により表示される認証画面を用いて認証モジュール１１７による認証が行われ、標準認証モードに設定されているアプリケーションに対してはシステム側認証制御部５０１により表示される認証画面Ａを用いてシステム側認証制御部５０１により認証が行われる。また、システム側認証制御部５０１と認証モジュール１１７間では、画面解放等に関する情報がやり取りされる。認証モジュール１１７により表示される認証画面の例を図２３に示す。この画面を認証画面Ｂと呼ぶ。

【０１１６】

次に、図２４に示すフローチャートを参照して、処理の流れを説明する。なお、以下の処理は、予め認証モジュールが優先アプリとして設定されている場合の例である。

【０１１７】

まず、複合機１００の電源ＯＮの後（ステップＳ３０１）、オペレーションパネルに認証モジュール１１７が認証画面Ｂを表示する（ステップＳ３０２）。ユーザーが、オペレーションパネルのアプリ切り替えキーを押下げることにより、利用したいアプリケーションを選択すると（ステップＳ３０３）、認証モジュール１１７は、認証モードの設定内容を確認し、選択されたアプリケーションが追加認証モードに対応するのか、もしくは標準認証モードに対応するのかを判断する（ステップＳ３０４）。

【０１１８】

選択されたアプリケーションが標準認証モードに対応する場合、当該アプリケーションは認証モジュール１１７の管理対象外なので、オペレーションパネルの画面表示部の制御

権限をシステム側認証制御部５０１に渡す（ステップＳ３０５）。これにより、システム側認証制御部５０１は認証画面Ａを表示する（ステップＳ３０６）。

【０１１９】

そして、システム側認証制御部５０１は、この画面から入力されるユーザーコードとパスワードを用いて認証を行い（ステップＳ３０７）、認証が成功であれば、選択されたアプリケーションの画面が表示され（ステップＳ３０８）、ユーザーによるアプリケーションの利用が可能になる。

【０１２０】

一方、選択されたアプリケーションが追加認証モードに対応する場合、当該アプリケーションは認証モジュール１１７の管理対象なので、既に表示されている認証モジュール１１７の認証画面Ｂから入力されたデータに基づき、認証モジュール１１７が認証を行う（ステップＳ３０９）。認証が成功であれば、選択されたアプリケーションの画面が表示され（ステップＳ３１１）、ユーザーによるアプリケーションの利用が可能になる。

【０１２１】

各アプリケーションの使用に際しては、第１の実施の形態で説明したように、印刷などのＪｏｂ完了、システムオートクリア等をトリガーとして、認証モジュール１１７の認証画面に戻る。

【０１２２】

また、システム側認証制御部５０１による認証画面Ａ、もしくはアプリケーションの画面が表示された状態で、別のアプリケーションへの切り替えが行われた場合、そのアプリケーションが認証モジュール１１７の管理対象であれば、切り替えが行なわれたときに認証モジュール１１７の認証画面Ｂに画面が遷移する。

【０１２３】

（第４の実施の形態）

次に、本発明の第４の実施の形態について説明する。

【０１２４】

これまでに説明した実施の形態では、ユーザーからのデータ入力を複合機１００のオペレーションパネルから行っていたが、ＰＤＡ(携帯情報端末：personal digital assistant)や、データ通信機能を持つ携帯電話から、認証のためのデータを入力することが可能である。本実施の形態では、ＰＤＡや携帯電話からデータを入力する場合について説明する。

【０１２５】

図２５に、複合機１００とＰＤＡ６０１、携帯電話６０２等が通信を行う場合の構成を示す。図２５に示すように、複合機１００はネットワーク６０３（ＬＡＮもしくはインターネット等のＷＡＮ）に接続される。接続は、有線でもよいし、無線ＬＡＮカード６０４を介して無線で行ってもよい。また、複合機１００に、アドホックネットワークを用いてＰＤＡ６０１と直接接続する機能を備えてもよい。更に、複合機１００に、携帯電話６０２と内線により通信できる機能を備えてもよい。

【０１２６】

また、複合機１００は、データ通信プロトコル処理機能６０５、Ｗｅｂサーバ機能６０６、認証画面データを生成する画面データ生成機能６０７を備える。なお、画面データ生成機能６０７は例えば認証モジュール１１７に備えられる。その他の複合機１００の構成は、これまでの実施の形態で説明したものと同様である。このような構成により、ＰＤＡ６０１や携帯電話６０２と複合機１００との間でデータ通信を行うことができる。以下、認証時の動作を説明する。以下の説明においては、ＰＤＡ６０１、携帯電話６０２を総称して携帯端末と呼ぶ。

【０１２７】

まず、複合機１００のＵＲＬもしくはＩＰアドレスを指定することにより、携帯端末が複合機１００にアクセスする。アクセスを受けた複合機１００は、認証に必要な情報を要求する画面に対応するＨＴＭＬデータもしくはＸＭＬデータを生成し、それを携帯端末に

返す。

【０１２８】

画面のデータを受信した携帯端末は図２０もしくは図２３に示すような画面を携帯端末の画面表示部に表示する。そして、携帯端末のユーザーが、必要な認証データを入力して複合機１００に対してそのデータを送信する。

【０１２９】

なお、携帯端末に認証データを一度登録しておけば次回からの操作が簡単になる。また、携帯電話と複合機１００が内線で通信を行う場合、予め複合機１００に内線番号を割り振り、複合機１００に発呼する際に、認証データを付加して送るようにすれば、更に簡単に認証作業を行なうことができる。

【０１３０】

認証データを受信した複合機１００は、例えば第３の実施の形態で説明した方法により認証を行い、認証が成功であれば複合機１００の画面がアプリケーションの画面に切り替わり、当該アプリケーションが使用可能となる。なお、アプリケーションの選択は複合機１００側で行ってもよいし、携帯端末から行ってもよい。

【０１３１】

本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【図面の簡単な説明】

【０１３２】

【図１】複合機の外観例と、オペレーションパネルを示す図である。

【図２】複合機１００と認証・課金サーバ１５０とがネットワークを介して接続された構成を示す図である。

【図３】複合機１００の構成を示すブロック図である。

【図４】複合機１００の構成を示すブロック図である。

【図５】複合機１００のハードウェア構成図である。

【図６】複合機１００の立ち上げ時の動作を示すフローチャートである。

【図７】アプリ設定ファイルを説明するための図である。

【図８】アプリ設定ファイルの内容例を示す図である。

【図９】ＳＣＳ１２２の起動後の複合機１００の動作を示すフローチャートである。

【図１０】優先アプリの設定を説明するための図である。

【図１１】第１の実施の形態におけるオペレーションパネル２１０の画面状態遷移図である。

【図１２】第１の実施の形態における認証モジュールの動作を説明するためのシーケンスチャートである。

【図１３】第２の実施の形態における画面状態遷移図である。

【図１４】第２の実施の形態における複合機１００の処理の流れを説明するための構成図である。

【図１５】第２の実施の形態における複合機１００の処理の流れを説明するためのシーケンスチャートである。

【図１６】認証モジュール１１７の構成の一例を示す図である。

【図１７】認証モジュール１１７（Ｊａｖａ（登録商標）プログラム）を含むＪａｖａ（登録商標）実行環境１１８の構成例である。

【図１８】認証モードの設定内容を示す図である。

【図１９】第３の実施の形態のおける認証方法を説明するための図である。

【図２０】システム側認証制御部により表示される認証画面Ａである。

【図２１】システム側認証制御部による認証画面を利用する場合のフローチャートである。

【図２２】第３の実施の形態のおける認証方法を説明するための図である。

【図２３】認証モジュールにより表示される認証画面Ｂである。

【図２４】システム側認証制御部による認証画面と認証モジュールによる認証画面を利用する場合のフローチャートである。

【図２５】複合機１００とＰＤＡ６０１、携帯電話６０２等が通信を行う場合の構成を示す図である。

【符号の説明】

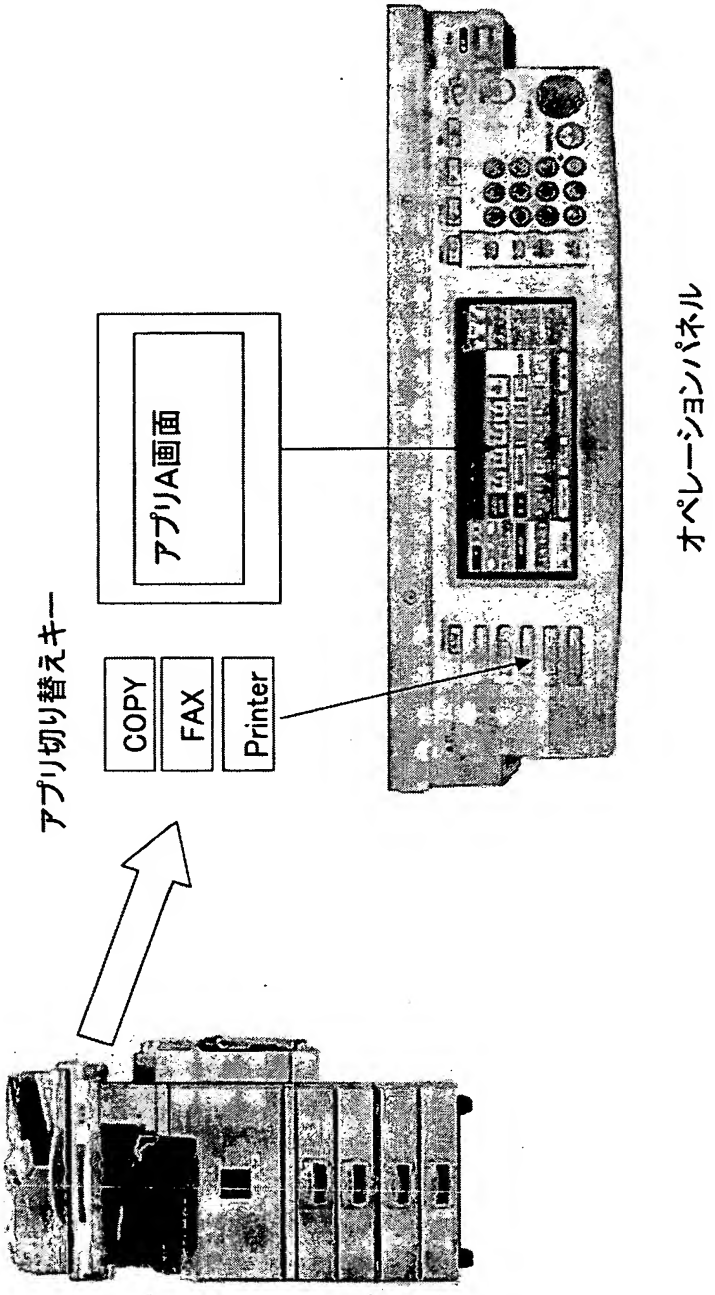
【０１３３】

１００ 複合機
１０１ 白黒ラインプリンタ
１０２ カラーラインプリンタ
１１０ ソフトウェア群
１１１ プリンタアプリ
１１２ コピーアプリ
１１３ ファックスアプリ
１１４ スキャナアプリ
１１５、１１６ 追加アプリ
１１７ 認証モジュール
１１８ Ｊａｖａ（登録商標）実行環境
１２０ プラットホーム
１２１ 汎用ＯＳ
１２２ ＳＣＳ
１２３ ＳＲＭ
１２４ ＥＣＳ
１２５ ＭＣＳ
１２６ ＯＣＳ
１２７ ＦＣＳ
１２８ ＮＣＳ
１３０ アプリケーション
１４０ 複合機起動部
１５０ 認証・課金サーバ
２００ コントローラボード
２０１ ＡＳＩＣ
２０２ ＣＰＵ
２０３ ＲＡＭ
２０４ ＲＯＭ
２０５ ＨＤＤ
２０６ フラッシュカードインタフェース部
２０７ フラッシュカード
２０９ ネットワークコントロールインターフェース
２１０ オペレーションパネル
２２０ ＦＣＵ
２３０ ＵＳＢ
２４０ ＩＥＥＥ１３９４
２５０ ブルートゥース
２６０ エンジン部
３０１ 認証制御部
３０２ 認証データ管理部
３０３ 利用制限管理部
３０４ 利用状況管理部
４００ Ｗｅｂサーバ
４０１ クラスライブラリ

４０２　仮想マシン
４０３　プログラムローダー
５０１　システム側認証制御部
６０１　ＰＤＡ
６０２　携帯電話
６０３　ネットワーク
６０４　無線ＬＡＮカード
６０５　データ通信処理機能
６０６　Ｗｅｂサーバ機能
６０７　画面データ生成機能

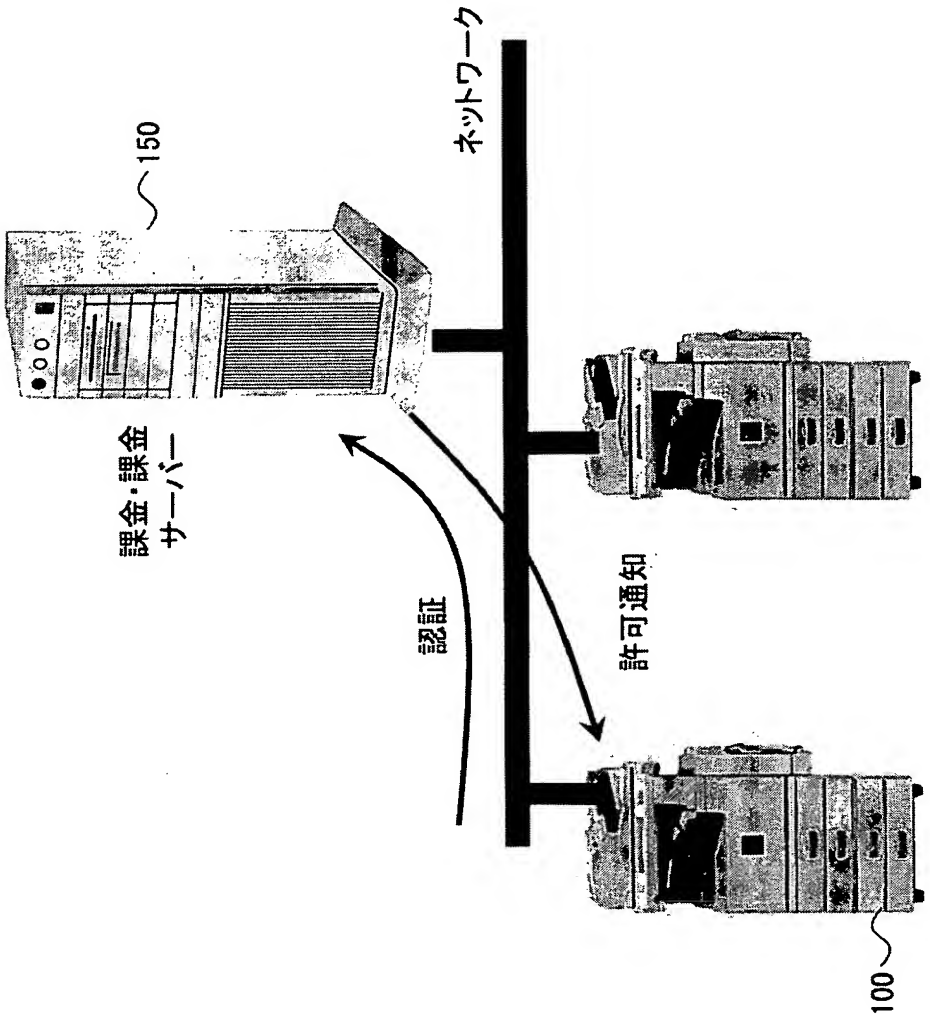
【書類名】図面
【図１】

複合機の外観例と、オペレーションパネルを示す図



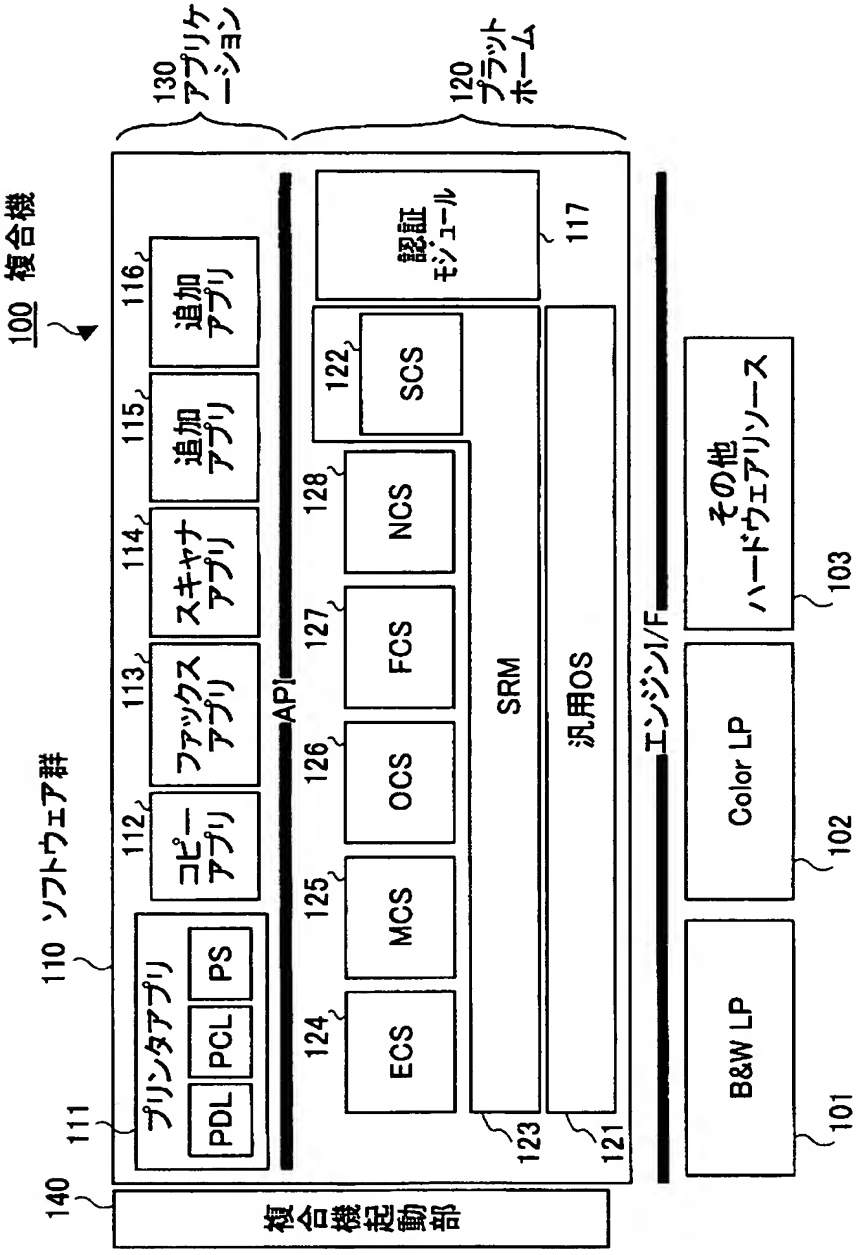
【図２】

複合機１００と認証・課金サーバ１５０とがネットワークを介して
接続された構成を示す図



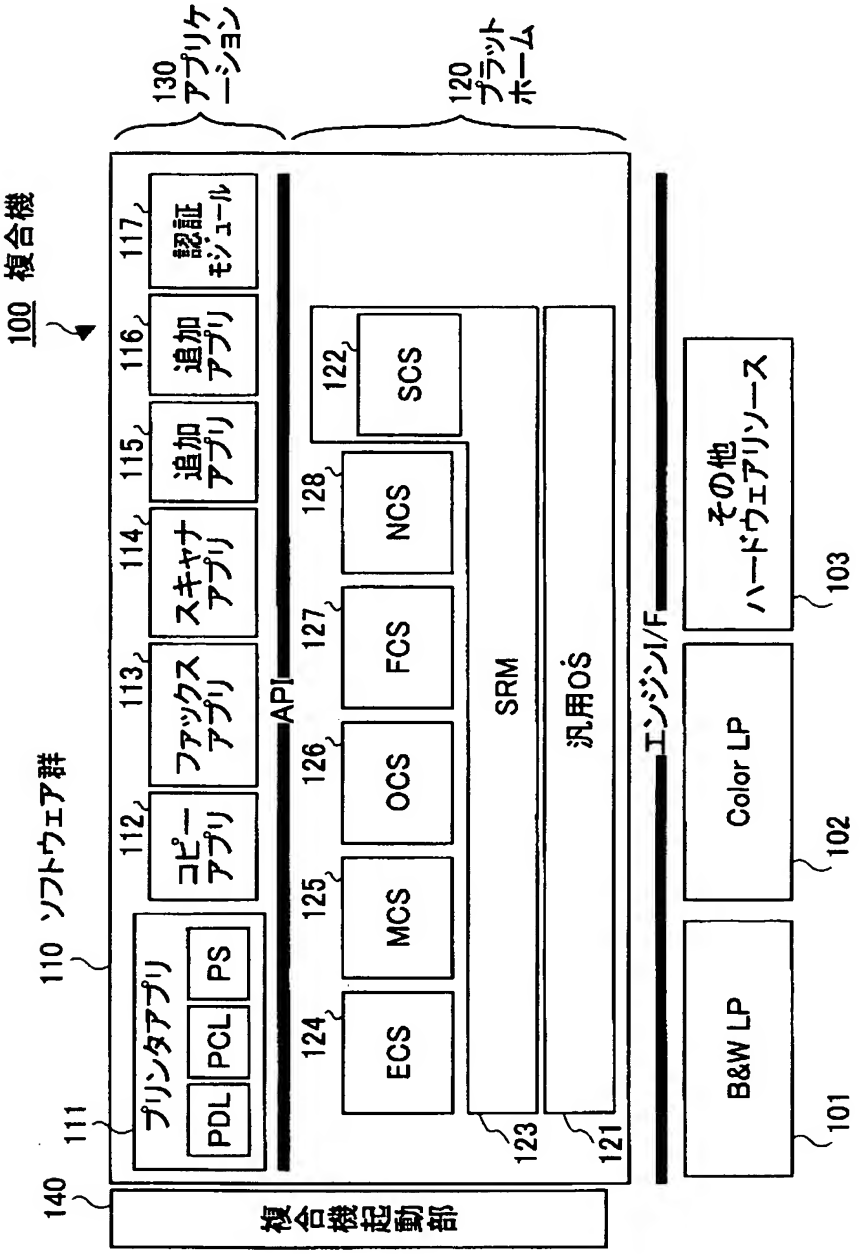
【図３】

複合機100の構成を示すブロック図



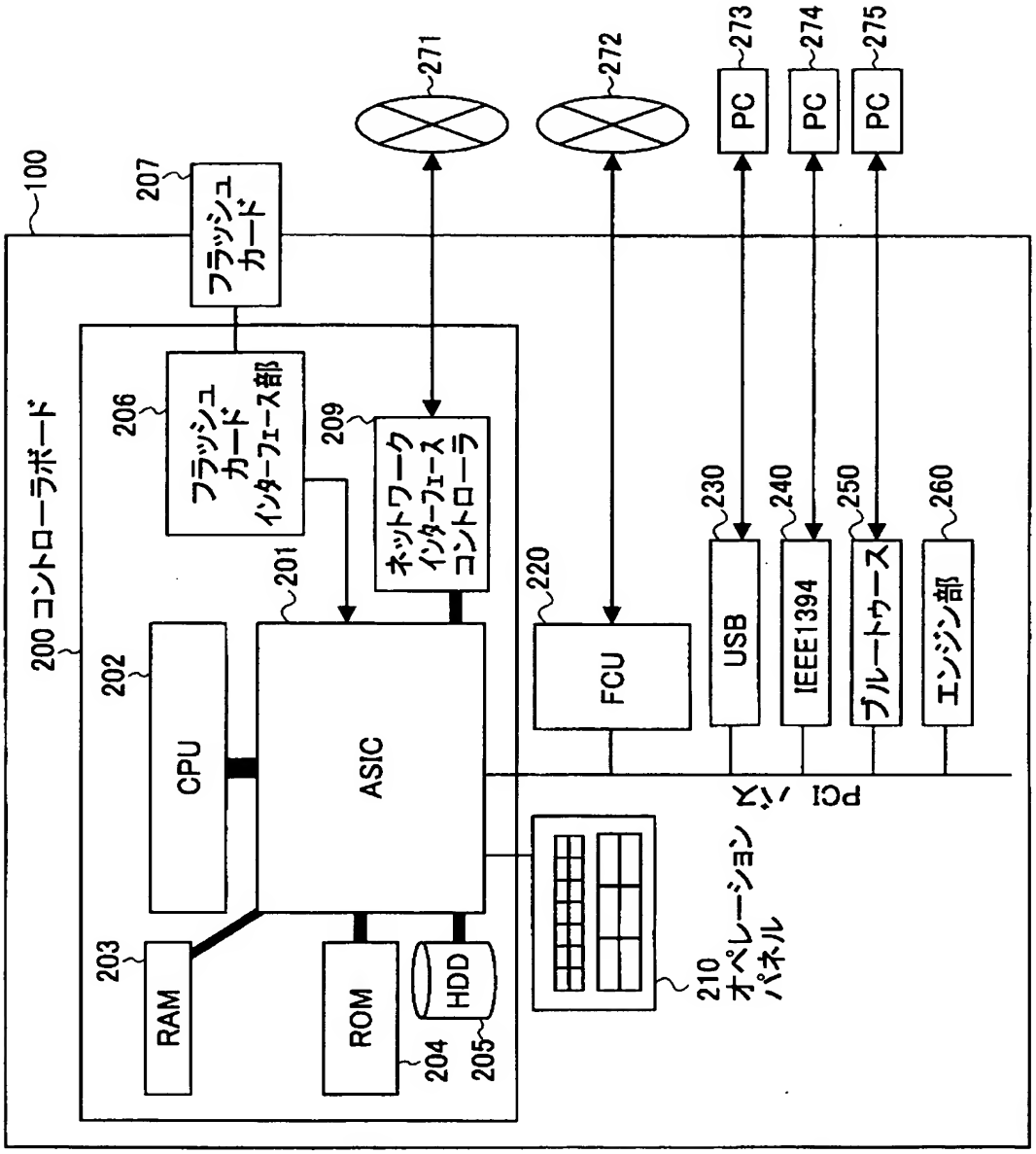
【図４】

複合機100の構成を示すブロック図



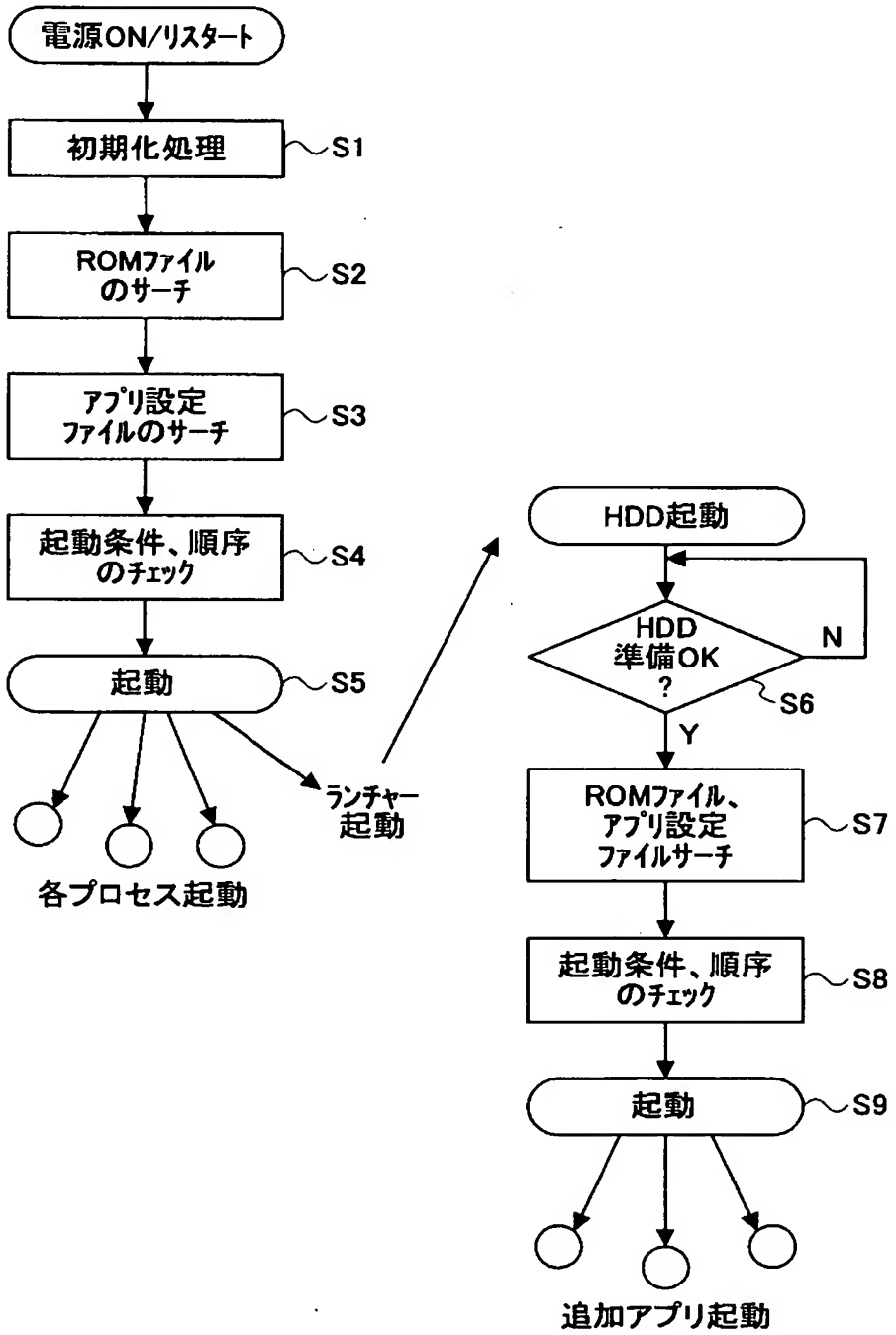
【図５】

複合機100のハードウェア構成図



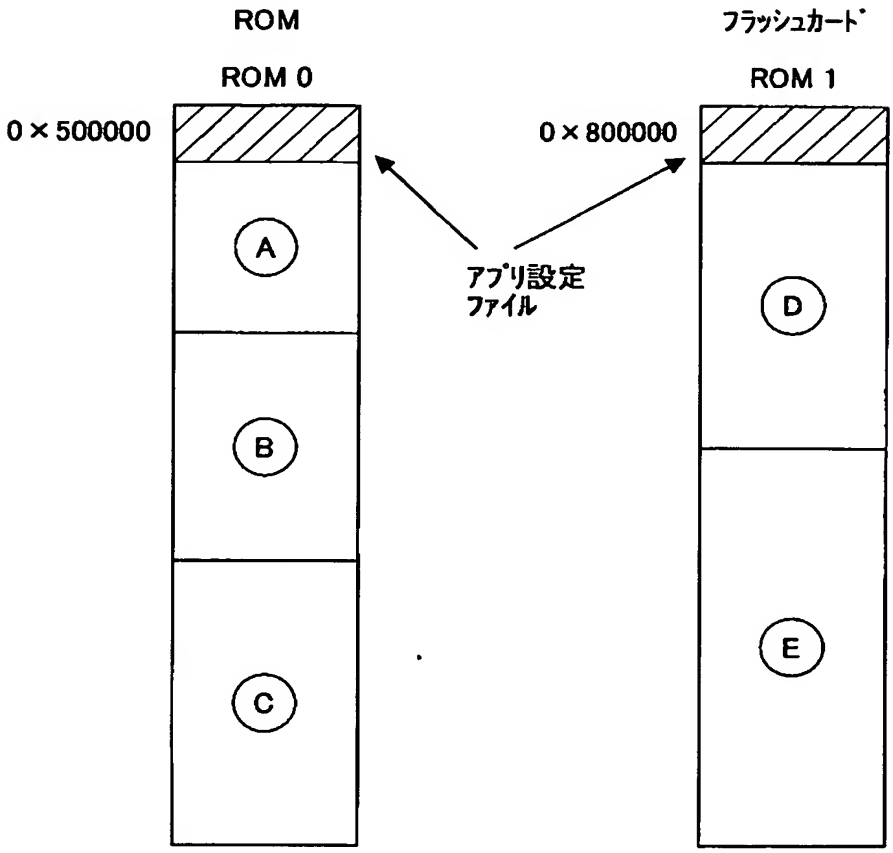
【図６】

複合機100の立ち上げ時の動作を示すフローチャート



【図７】

アプリ設定ファイルを説明するための図



【図８】

アプリ設定ファイルの内容例を示す図

(a)

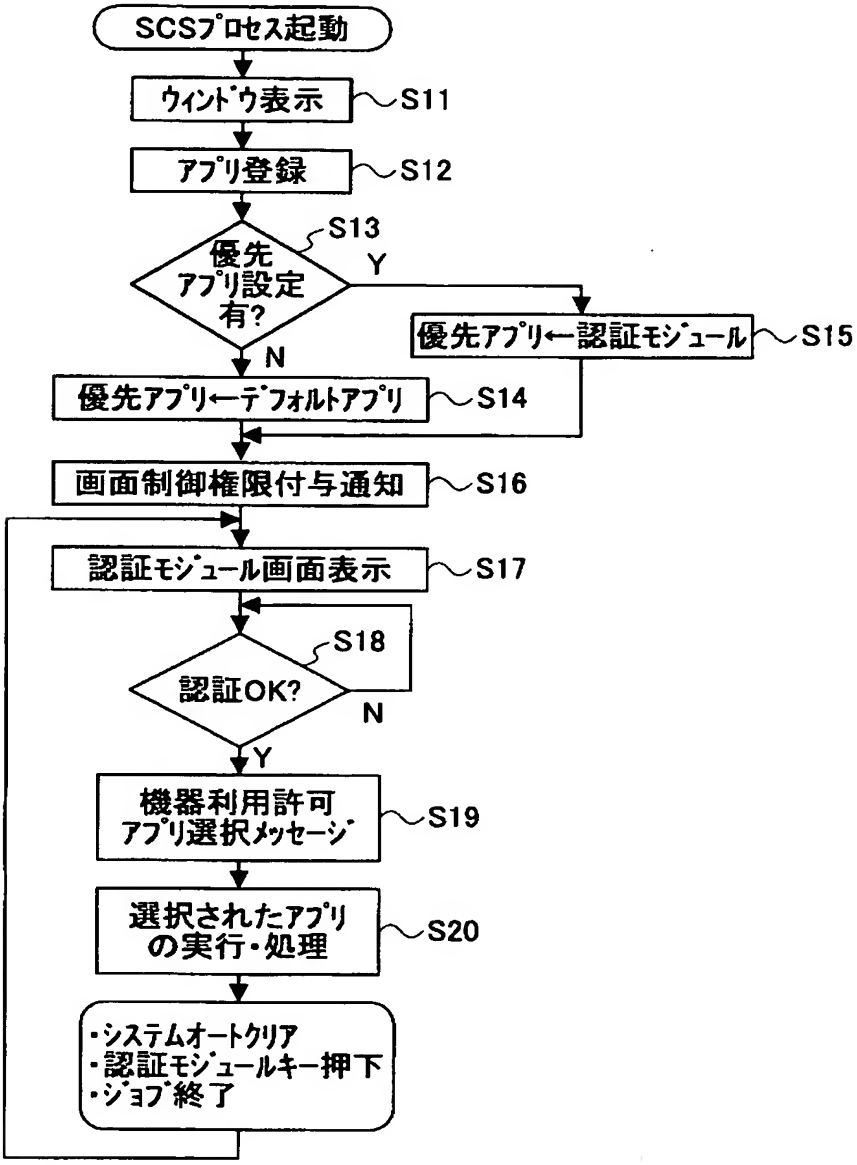
```
mount   romfs   0×500000   ROM 0
mount   romfs   0×800000   ROM 1
exec    -2      /bin/Ⓐ
exec    -5      /bin/Ⓑ
exec    -3      /bin/Ⓒ
```

(b)

```
exec    -2      /bin/Ⓓ
exec    -3      /bin/Ⓔ
```

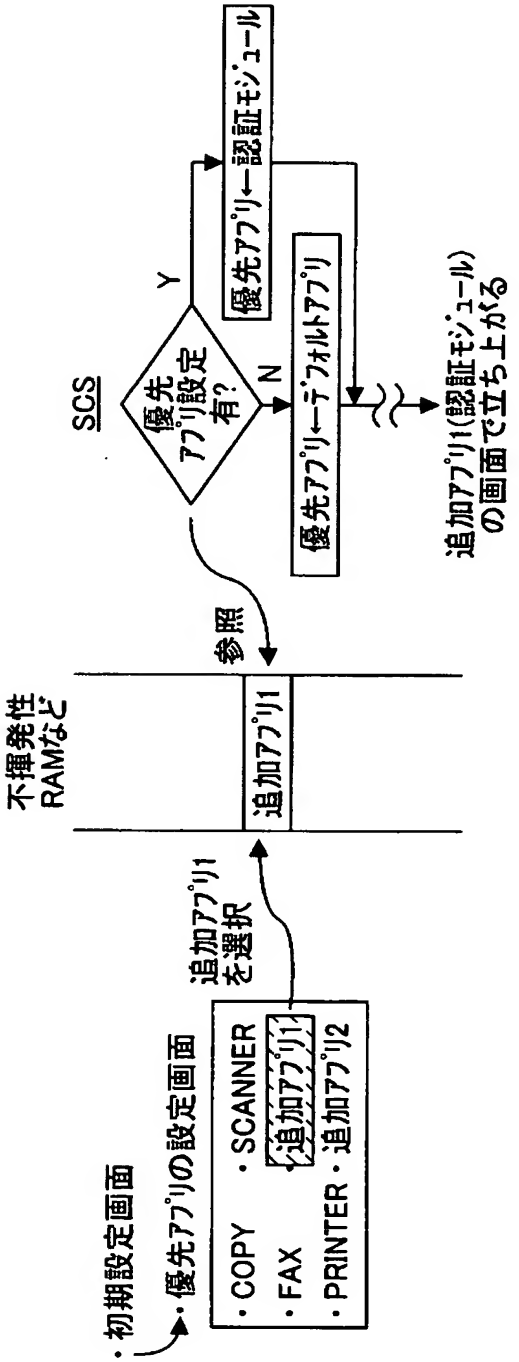
【図９】

SCS122の起動後の複合機100の動作を示すフローチャート



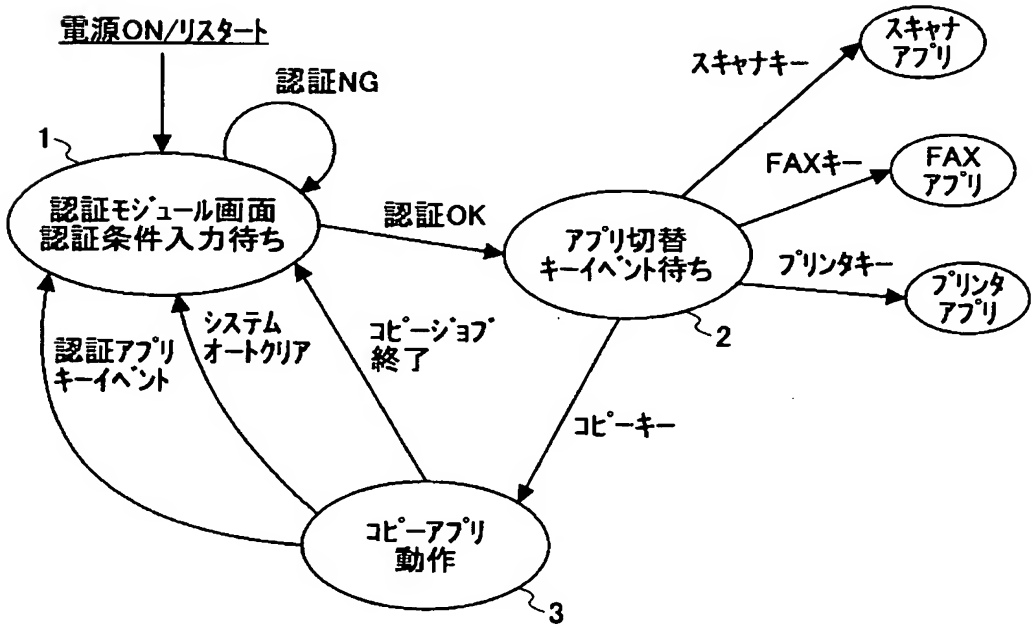
【図１０】

優先アプリの設定を説明するための図



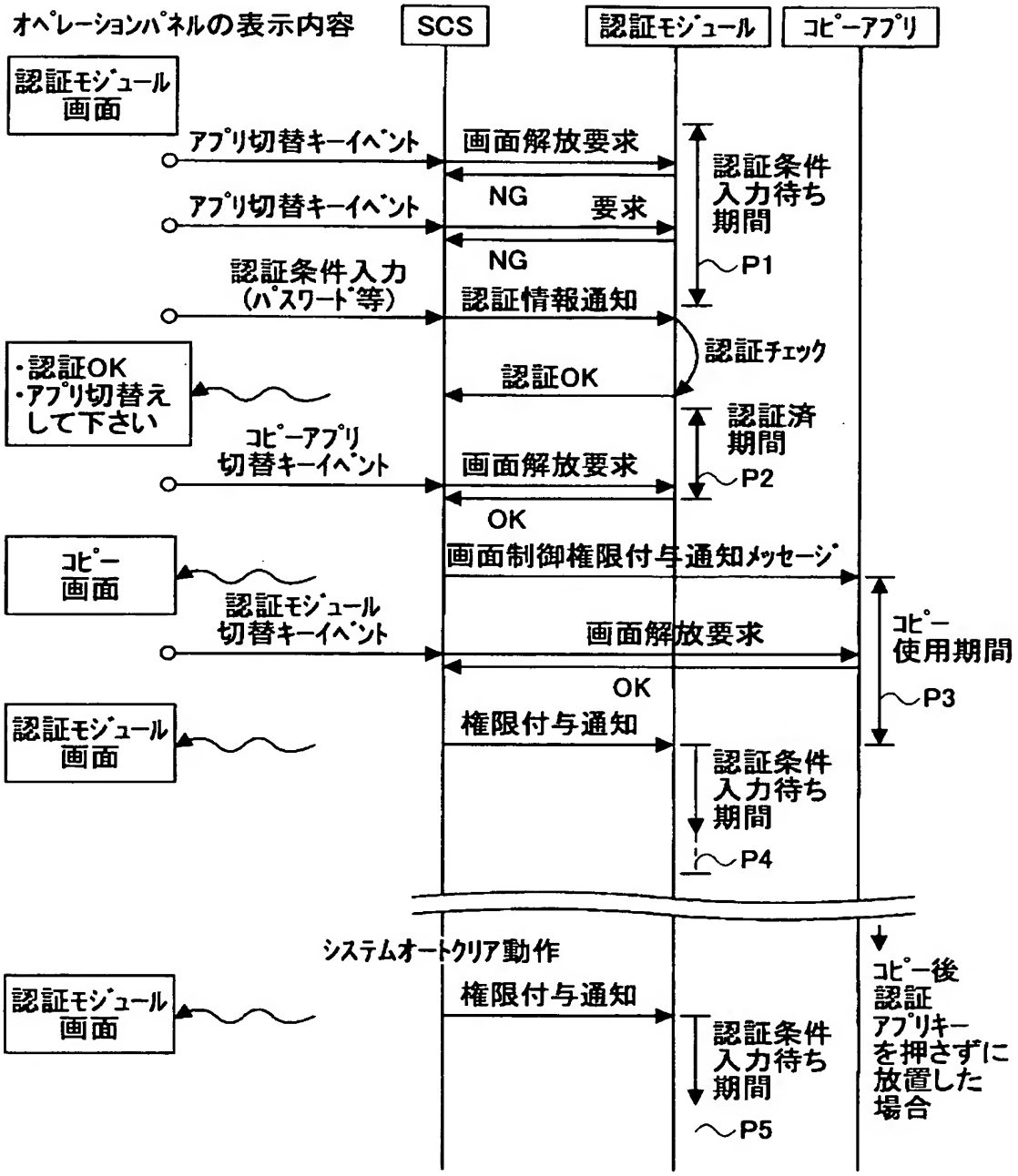
【図１１】

第１の実施の形態におけるオペレーションパネル２１０の
画面状態遷移図



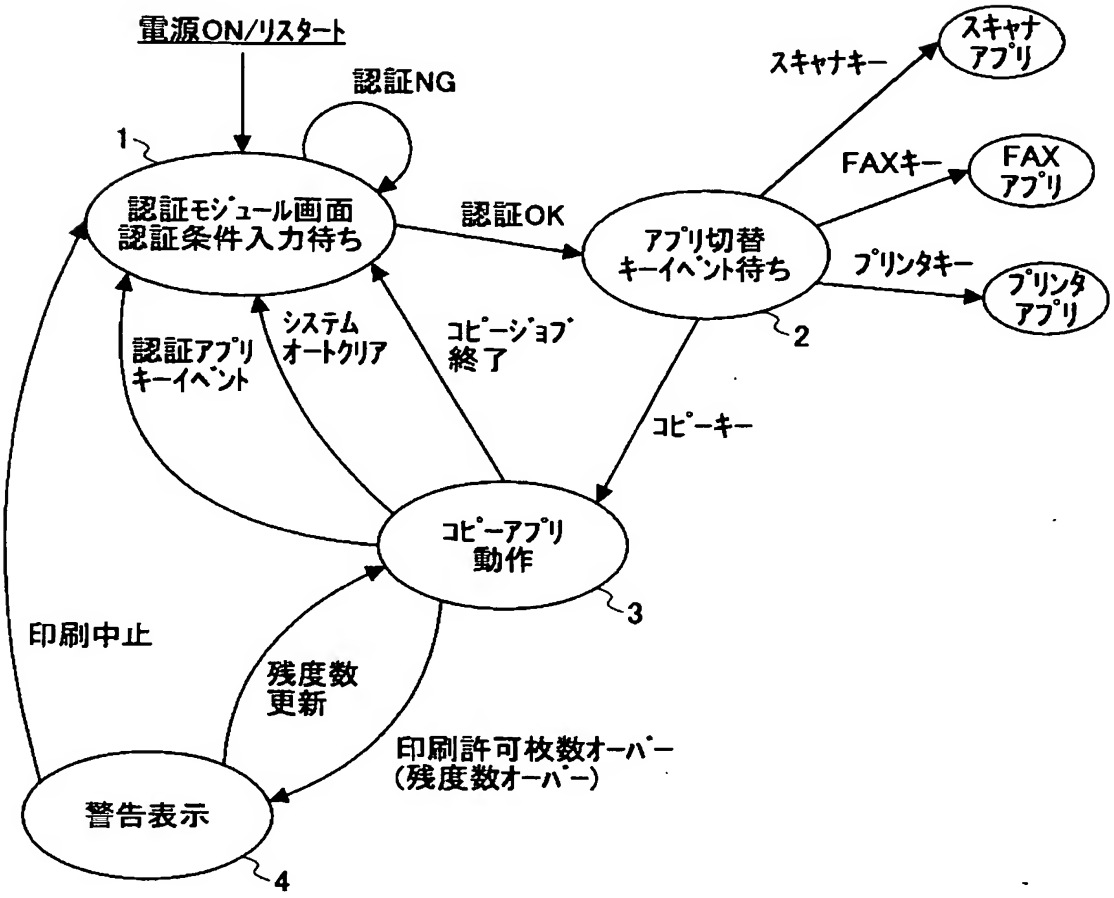
【図１２】

第１の実施の形態における認証モジュールの
動作を説明するためのシーケンスチャート



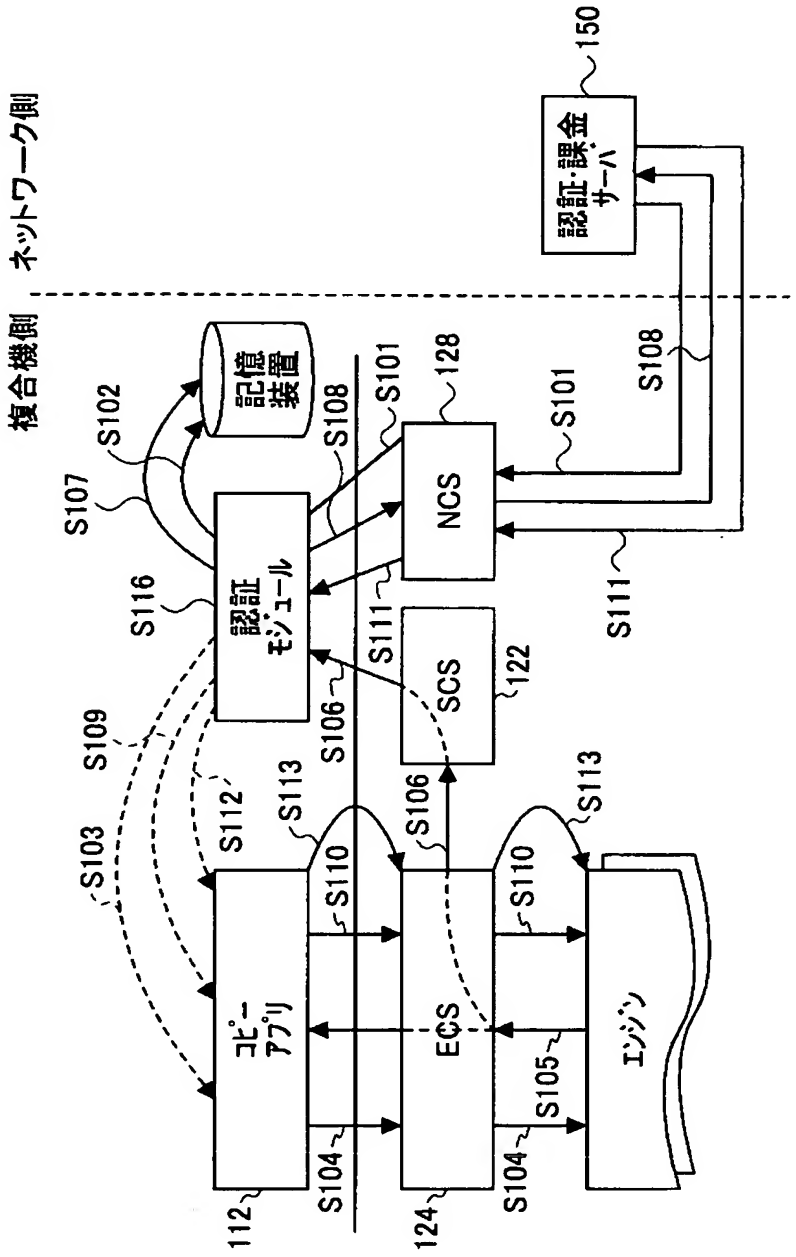
【図１３】

第2の実施の形態における画面状態遷移図



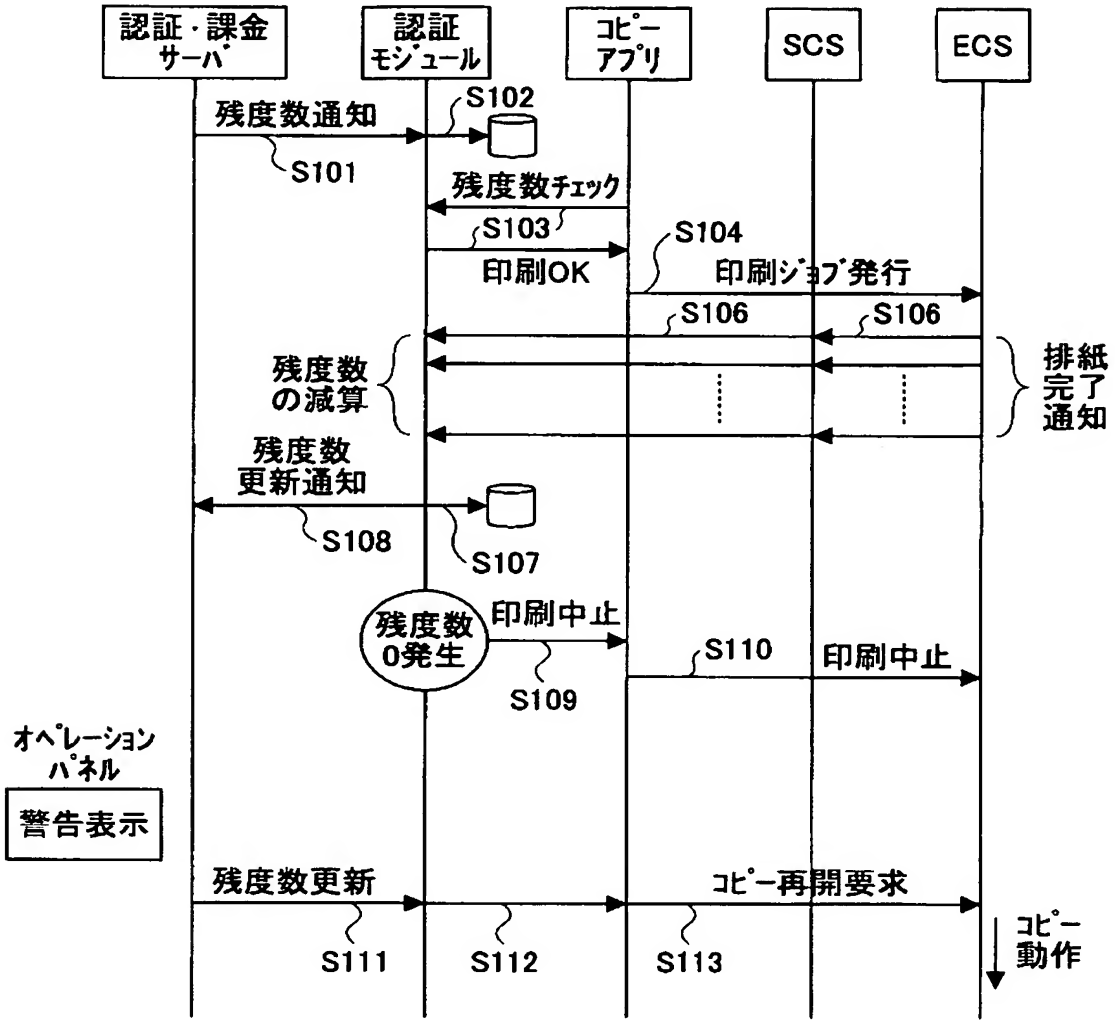
【図１４】

第2の実施の形態における複合機100の処理の流れを説明するための構成図



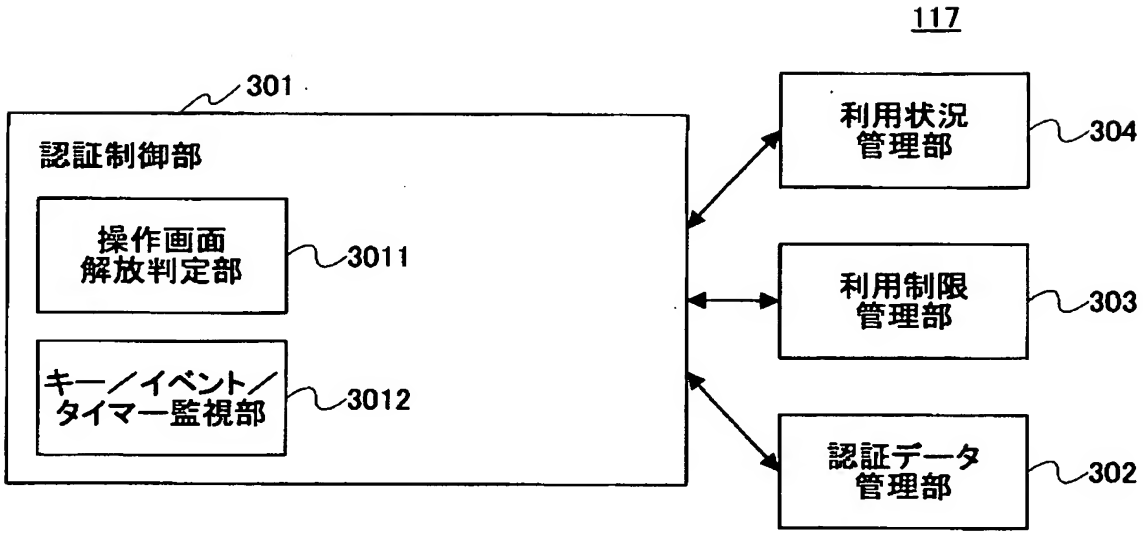
【図１５】

第2の実施の形態における複合機100の処理の流れを説明するためのシーケンスチャート



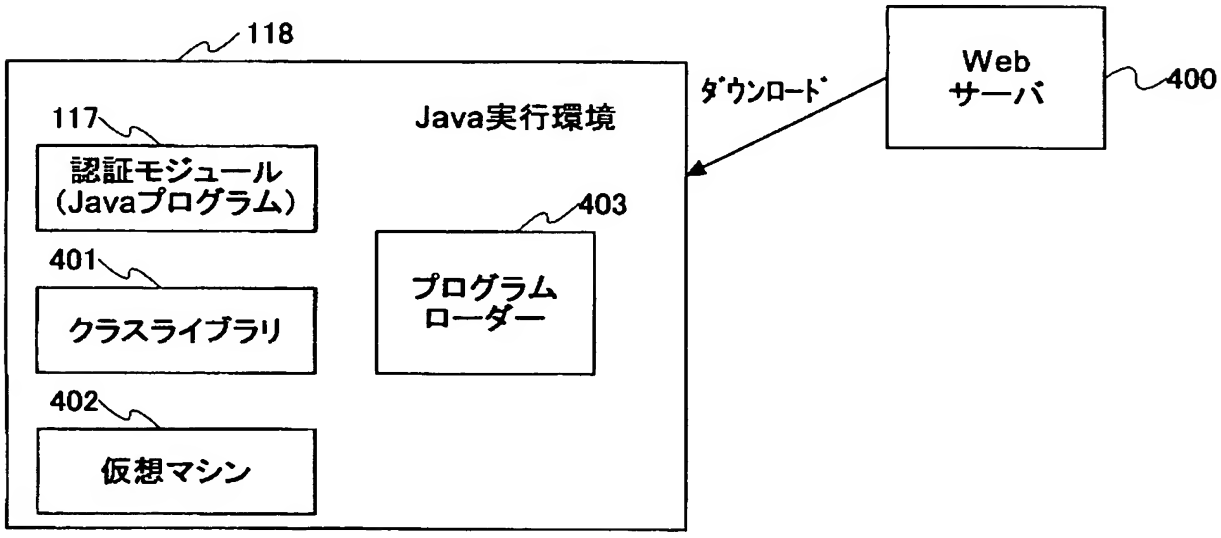
【図１６】

認証モジュール１１７の構成の一例を示す図



【図１７】

認証モジュール１１７（Ｊａｖａプログラム）を含む
Ｊａｖａ実行環境１１８の構成例



【図１８】

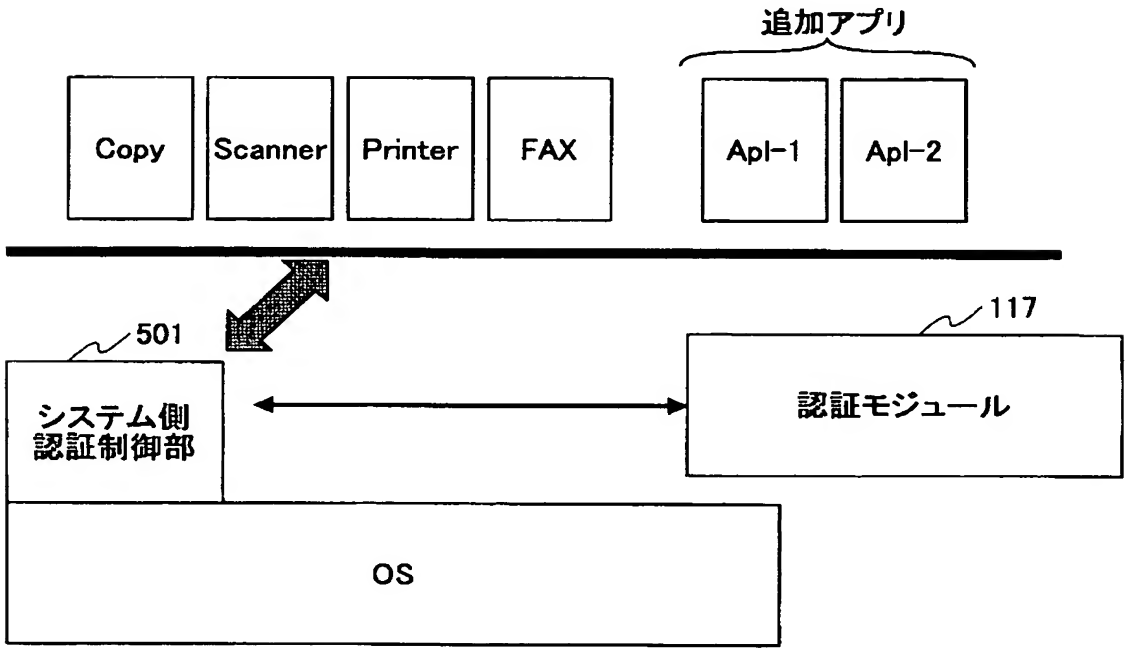
認証モードの設定内容を示す図

■システム設定

	利用制限 する／しない	認証モード
Copy	する	標準
スキャナ	する	追加
FAX	しない	－
追加アプリ1	する	追加
追加アプリ2	する	標準

【図１９】

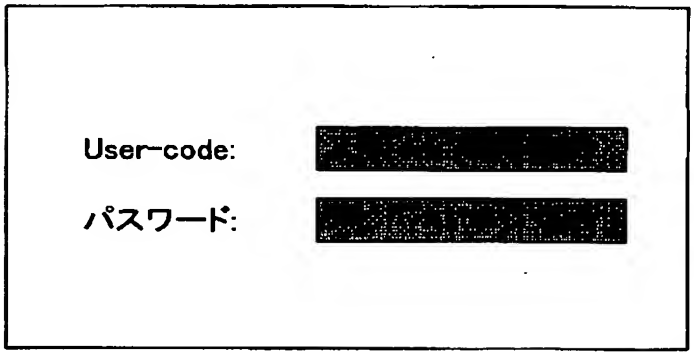
第３の実施の形態における認証方法を説明するための図



【図２０】

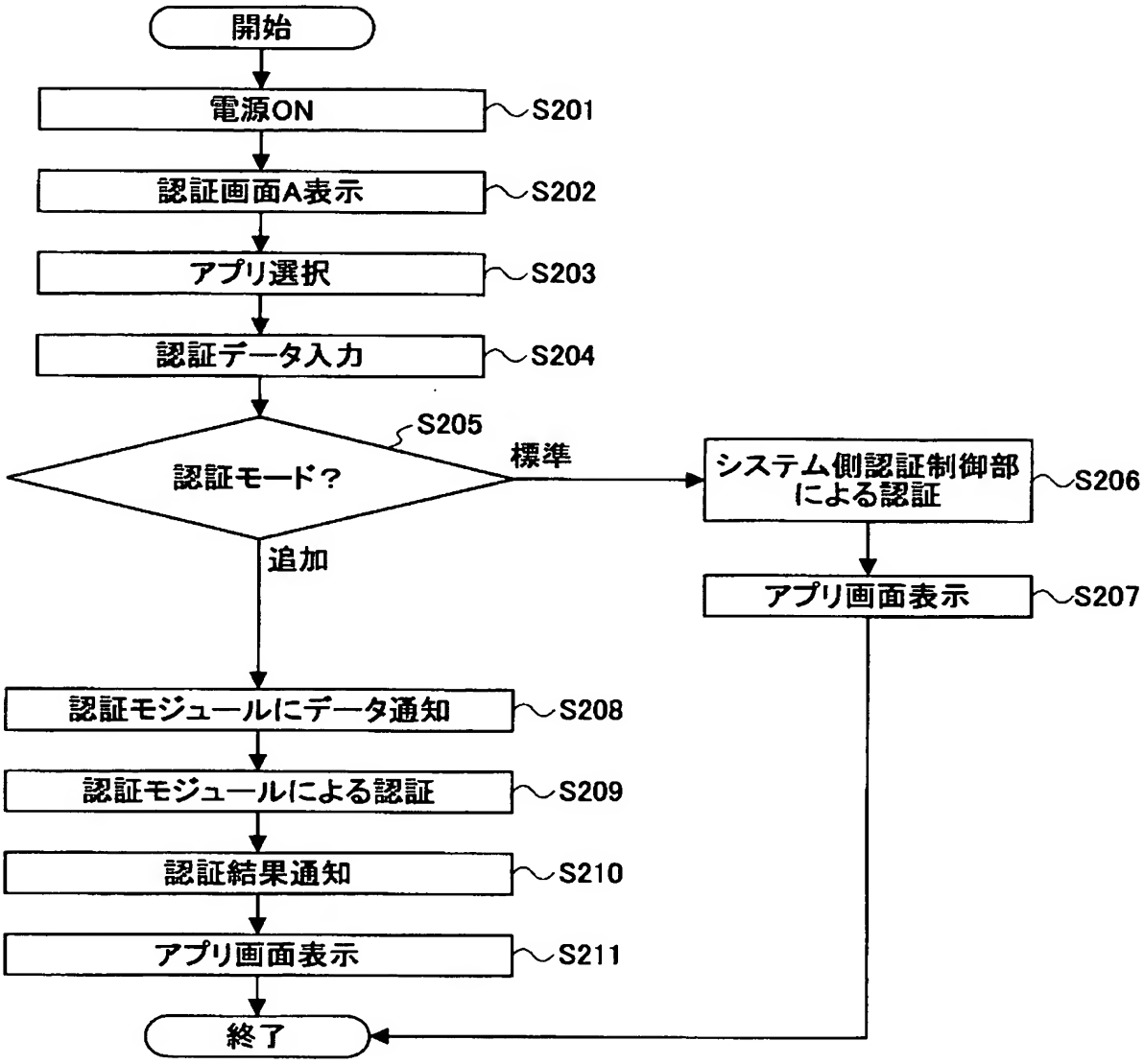
システム側認証制御部により表示される認証画面Ａ

認証画面 A



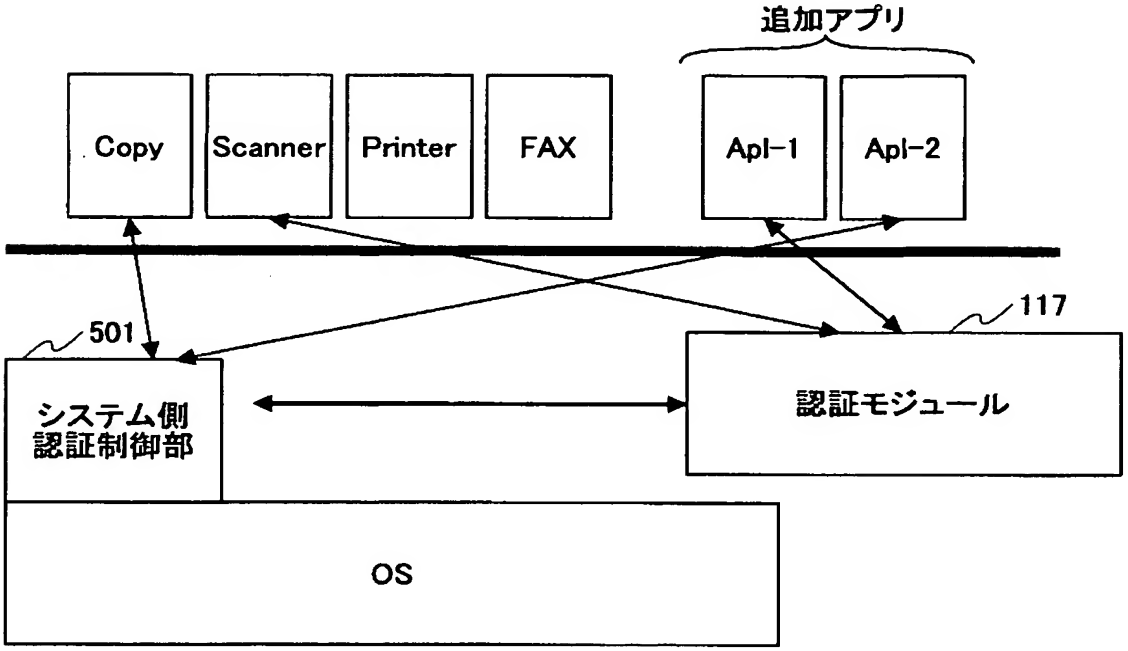
【図２１】

システム側認証制御部による認証画面を利用する場合のフローチャート



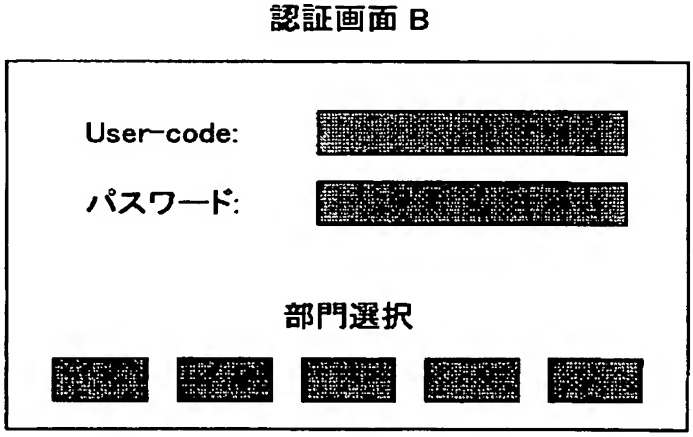
【図２２】

第３の実施の形態における認証方法を説明するための図



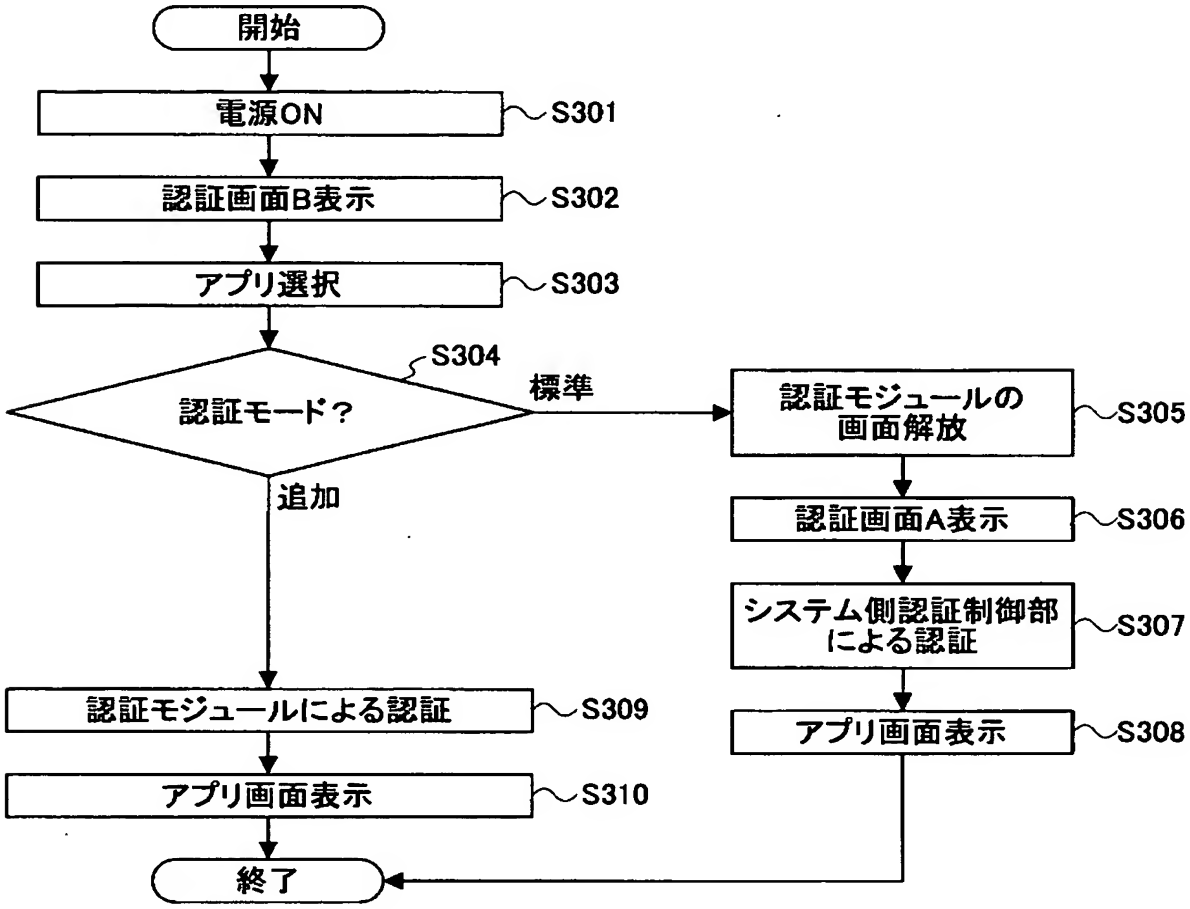
【図２３】

認証モジュールにより表示される認証画面Ｂ



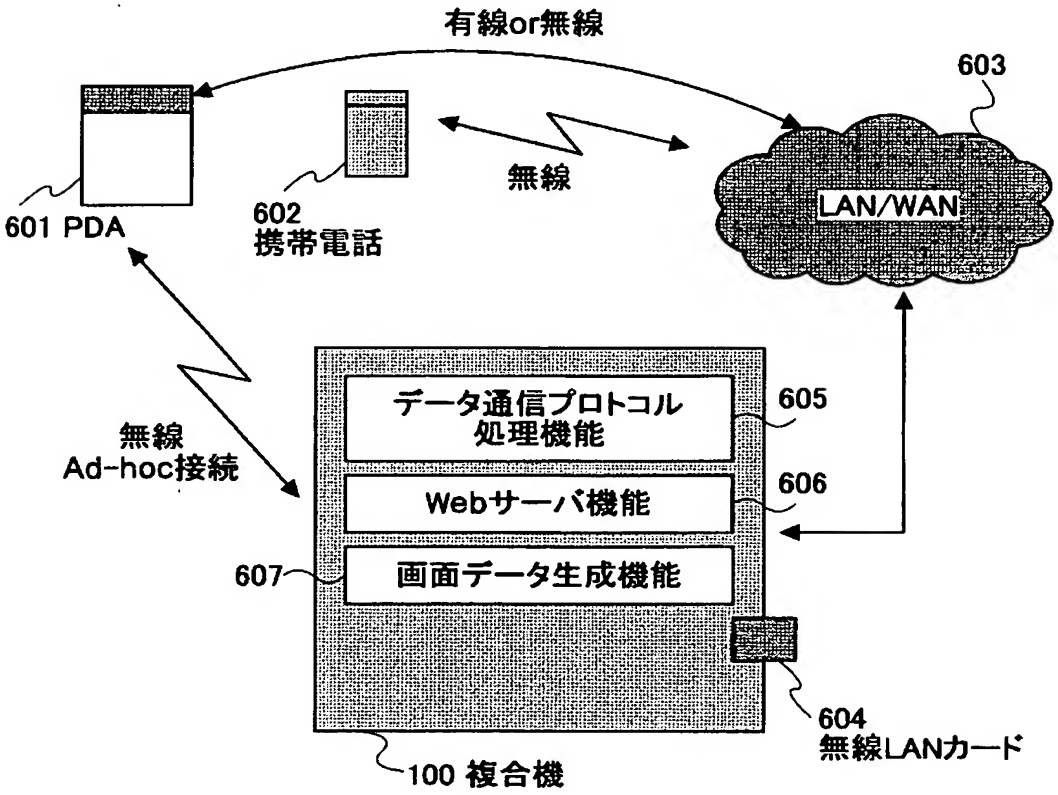
【図２４】

システム側認証制御部による認証画面と認証モジュールによる認証画面を利用する場合のフローチャート



【図２５】

複合機１００とＰＤＡ６０１、携帯電話６０２等が
通信を行う場合の構成を示す図



【書類名】要約書
【要約】
【課題】　種々の目的に応じた認証機能を容易に追加、変更することを可能とする。
【解決手段】アプリケーションと、当該アプリケーションにシステム側サービスを提供するシステム側ソフトウェアとを有する画像形成装置において、認証用画面を前記画像形成装置のオペレーションパネルに表示させ、前記認証用画面から入力された認証用データが認証条件を満たした場合に、画像形成装置の使用をするための画面を前記認証用画面に代えて前記オペレーションパネルに表示させる認証モジュールを有し、当該認証モジュールを前記システム側ソフトウェアとは別に備えるように構成した。
【選択図】　図３

特願２００４－０１２９０４

出　願　人　履　歴　情　報

識別番号　［０００００６７４７］

１．変更年月日　２００２年　５月１７日
［変更理由］　住所変更
住　所　東京都大田区中馬込１丁目３番６号
氏　名　株式会社リコー